(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年7月5日 (05.07.2001)

PCT

(10) 国際公開番号
WO 01/48755 A1

(51) 国際特許分類[7]: G11B 20/10, 20/12, G06F 17/60, 3/06, H04N 5/91, H04L 9/00

(21) 国際出願番号: PCT/JP00/09260

(22) 国際出願日: 2000年12月26日 (26.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/375777 1999年12月28日 (28.12.1999) JP
特願2000/247688 2000年8月17日 (17.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).

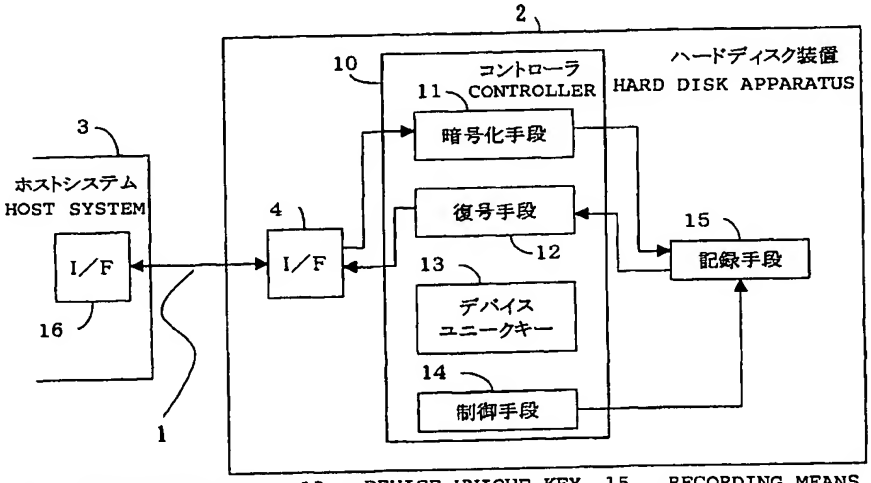
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 吉田修一 (YOSHIDA, Shuichi) [JP/JP]; 〒555-0024 大阪府大阪市西淀川区野里2-7-25 Osaka (JP). 岡田孝文 (OKADA, Takanori) [JP/JP]; 〒560-0045 大阪府豊中市刀根山6-5-76-102 Osaka (JP). 久野良樹 (KUNO, Yoshiki) [JP/JP]; 〒570-0054 大阪府守口市大枝西町14-26-204 Osaka (JP). 米野潤一 (KOMENO, Jyun-ichi) [JP/JP]; 〒536-0001 大阪府大阪市城東区古市3-1-2-1202 Osaka (JP). 神門俊和 (KOUDO, Toshikazu) [JP/JP]; 〒663-8102 兵庫県西宮市松並町13-5-302 Hyogo (JP). 清水亮輔 (SHIMIZU, Ryosuke) [JP/JP]; 〒573-1111 大阪府枚方市楠葉朝日3-10-31 Osaka (JP). 久保徳章 (KUBO, Noriaki) [JP/JP]; 〒560-0045 大阪府高槻市月見町3-1-508 Osaka (JP).

(74) 代理人: 弁理士 松田正道(MATSUDA, Masamichi); 〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka (JP).

[続葉有]

(54) Title: RECORDING APPARATUS, REPRODUCING APPARATUS, DATA PROCESSING APPARATUS, RECORDING/REPRODUCING APPARATUS, AND DATA TRANSMITTING APPARATUS

(54) 発明の名称: 記録装置、再生装置、データ処理装置、記録再生装置、データ送信装置



11...ENCRYPTING MEANS 13...DEVICE UNIQUE KEY 15...RECORDING MEANS
12...DECRYPTING MEANS 14...CONTROL MEANS

(57) Abstract: There has been conventionally no concrete contrivance to protect copyright when AV data is recorded in a recording apparatus and/or when data is reproduced by a reproducing apparatus. A recording apparatus comprising encrypting means (11) for encrypting AV data sent from an interface (4), control means (14) for control to record encrypted AV data, recording means (15) controlled by the control means (14) so as to record encrypted AV data on a magnetic disk, wherein the control means (14) carries out control to reproduce recorded data, the recording means (15) is controlled by the control means (14) and reproduces data recorded on a disk, and decrypting means (12) decrypts the reproduced data and sends it to an interface.

[続葉有]

WO 01/48755 A1

WO 01/48755 A1

(81) 指定国 (国内): CN, JP, KR, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(57) 要約:

ＡＶなどのデータを記録装置に記録する場合及び／またはデータを再生装置で再生する場合に著作権を保護する具体的な仕組みがない。

インターフェース４から送られてくるＡＶデータを暗号化する暗号化手段１１と、暗号化されたＡＶデータを記録するよう制御する制御手段１４と、制御手段１４によって制御され、暗号化されたＡＶデータを磁気ディスクに記録する記録手段１５とを備え、制御手段１４は、記録されたデータを再生するよう制御し、記録手段１５は制御手段１４によって制御され、ディスクに記録されたデータを再生し、復号手段１２は、再生されたデータを復号してインターフェースに送る。

明　細　書

記録装置、再生装置、データ処理装置、記録再生装置、データ送信装置

技術分野

本発明は、データを記録する記録装置、データを再生する再生装置、記録媒体に記録されているデータを他の装置へ移動させるまたは複写するデータ処理装置、そのように移動してきたデータを記録し再生する記録再生装置、複数個のデータで構成されているストリームを送信するデータ送信装置、テレビ放送等にて放送されるコンテンツを、所定の時間遅らせて視聴するタイムシフト再生を行うための記録装置と記録再生装置に関するものである。

背景技術

新作の映画や有料放送のテレビ番組、音楽などの著作権保護が必要なデータを扱う場合、著作権を保護することが必要である。著作権を保護するための有力な方法として、著作権を保護する必要があるデータを暗号化してデータの利用に制限を加える方法がある。

例えば、映像音声データ（以下ＡＶデータと記す）を伝送する際、ＡＶデータを著作権保護する必要がある場合、そのＡＶデータを暗号化して伝送することが行われている。そのような例としてＩＥＥＥ１３９４－ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｐｒｏｔｅｃｔｉｏｎ）方式が規格化されている。

ＩＥＥＥ１３９４は、シリアル伝送を行う高速バスシステムで、データを同期伝送できるため、ＡＶデータなどのリアルタイム伝送が可能である。このようなＩＥＥＥ１３９４は、家庭用ディジタルＡＶ機器を始め、多くのディジタル映像音声機器に外部用インターフェースとして搭載されようとしている。

ＩＥＥＥ１３９４－ＤＴＣＰ方式によれば、ＩＥＥＥ１３９４バスでデータ伝送する際に、認証機能と鍵の無効化機能を備えており、ＡＶデータなどの著作権保護が必要なデータを暗号化して伝送することにより著作権の保護を実現することが出来る。

さて、パーソナルコンピュータの普及と進歩に伴い、外部記憶装置としてその大容量性、高速性からハードディスク装置などの記録装置や再生装置が数多く用いられている。さらに、最近ハードディスク装置は、コンピュータのみならず、デジタル技術を応用して映像、音声を記録再生するデジタルＡＶ機器などにもその高速性、大容量性を生かして用いられつつある。

このように従来から映画の創作者等は、自ら作成したデータを第三者に勝手にコピーさせたくないと考える場合がある。そこで、著作権を保護するために、他の記録媒体へのコピーをすることが禁止されているデータや、１回のみのコピーだけが許されているデータというものが存在する。

そのようなデータは、例えばＨＤＤにコピーして蓄積された場合であれば、そのＨＤＤにおいてのみ再生されるということになる。

また、テレビ放送の視聴法の１つとして、放送された番組（コンテンツ）を一時的にＶＴＲ等の記録装置に記録しておき、記録したデータを後に再生することにより、本来の放送時刻と異なる時刻に番組を視聴することは従来より盛んに行われている。

特に、記録装置に、ハードディスク等の、ランダムアクセス可能であり、記録再生が同時に可能な記録媒体を用いた場合は、従来のテープ媒体を用いたＶＴＲに対し、番組の放送時間内であるわずかな時間だけ遅れた後にでも、当該番組の内容を欠かすことなく連続して視聴することができるなどの、狭義のタイムシフト再生を実現することができる。

図４３は、従来の技術による、タイムシフト再生を実現するための記録再生装置の構成図である。図に示すように、記録再生手段２１２０は、外部からの放送を記録再生するための手段、記録媒体２１３０は、ハードディスク等で実現される、放送のデータを蓄積するための手段、切り替え手段２１６０は、記録再生手段２１２０からの入力と、外部からの放送の入力とを受け、いずれかを選択して外部のモニタ等へ出力する手段である。

このような構成を有する従来の技術による記録再生装置の動作の一例を以下に説明する。

はじめに、視聴者が、リアルタイムで番組を視聴している場合、切り替え手段２１６０は、外部からの放送をそのままモニタへ出力するよう設定する一方で、記録再生手段２１２０は、同一の番組内容を記録媒体２１３０へ記録している。

次に、視聴者が、一時的にモニタの前を離れた後、再びモニタの前に戻り、番組の視聴を再開する場合は、記録再生手段２１２０は、視聴者がモニタの前を離れた時点から、記録したデータを再生し、切り替え手段２１６０は記録再生手段２１２０からの入力をモニタへ出力するように設定する。これ以後、視聴者は、番組として、記録再生手段２１２０からの再生出力を視聴することになる。

上記の動作において、記録再生手段２１２０は、データを再生する一方で、外部からの放送の録画も平行して行う。すなわち、記録再生手段２１２０は、データの再生と記録を同時に行っている。

これにより、視聴者は、リアルタイムで放送されている番組を視聴する際に、一時的に視聴を中断しなければならないような場合でも、視聴の中断時間だけ遅れて、番組の内容を切れ目無く把握しつつ視聴することが可能となる。

ところが、ＡＶデータを伝送する場合と同様に、著作権保護を必要とするＡＶデータをハードディスク装置などの記録媒体に記録する場合及び／または再生する場合にも著作権を保護する仕組みが必要である。ところが、記録装置及び／または再生装置に著作権保護を必要とするＡＶデータを記録及び／または再生する場合にどのようにして著作権を保護するかは具体的に決定されていない。

また、ＡＶデータに限らず、インターネットなどから送られてくる文書データや、ゲームソフトなどのコンピュータプログラムについてもＡＶデータと同様に著作権保護を必要とする場合がある。しかしながら、記録装置及び／または再生装置に著作権保護を必要とするこのようなデータを記録及び／または再生する場合にどのよにして著作権を保護するかは具体的に決定されていない。

すなわち、ＡＶデータや文書データやコンピュータプログラムなどのデータを記録装置に記録する場合及び／またはこれらのデータを再生装置で再生する場合に著作権を保護する具体的な仕組みがないという課題がある。

また、上記のＨＤＤのデータ記録残存容量が少なくなってくると、ＨＤＤに記録されているデータの上に新たなデータを上書きしたり、ＨＤＤに記録されている一部のデータを削除して残存容量を増やす必要がでてくる。しか

しながら、ＨＤＤのユーザは、ＨＤＤに記録されているデータへの上書きや、データの削除をしたくないと考え、ＨＤＤに記録されているデータを他の記録媒体にコピーしたいと考える場合がある。

他方、上述したように著作権者は、ＨＤＤに記録されたデータを著作権を無視してコピーされると困る。

すなわち、著作権保護が必要なデータをＨＤＤなどの記録装置に記録している場合、ユーザは、そのデータを他の記録媒体にコピーすることが出来ないという課題がある。

また、ケーブルテレビやＣＳ放送等の、放送形態の多様化、信号のデジタル化等により、放送される番組にも著作権上の問題が考慮され、信号にコピーガードを含むことにより、複製のための記録があらかじめ不可能に設定された番組の放映が実現されている。

しかしながら、従来の記録再生装置において、上述のような著作権を考慮した番組に対してタイムシフト再生を実現するためには、記録媒体２１３０に番組を記録することが、番組に関する著作権の侵害を引き起こす恐れがあるという問題があった。

すなわち、著作権保護が必要な番組についてタイムシフト再生を実現すると、番組に関する著作権の侵害を引き起こす恐れがあるという課題がある。

このような問題を回避する方策としては、（１）タイムシフトが可能な時間を制限する。（２）放送されるコンテンツが丸ごと保存されることを防ぐ等の方法が考えられる。

発明の開示

本発明は、上記課題を考慮し、著作権保護が必要なデータを記録する場合及び／または著作権保護が必要なデータを再生する場合に著作権を保護することが出来る記録装置及び再生装置を提供することを目的とするものである。

また、本発明は、上記課題を考慮し、著作権を保護しつつ、コピーが禁止されているデータを他の記録媒体に移動させるまたは複写するデータ処理装置と、そのデータ処理装置からのデータを記録媒体に記録し、または記録するとともに再生する記録再生装置と、著作権を保護してデータをバックアップしておく暗号化データ復号記録装置システムおよびそのシステムを構成する復号記録装置、記録装置と、著作権を保護してデータを送信するデータ送信装置とを提供することを目的とするものである。

また、本発明は、上記課題を考慮し、本来の放送時間より遅れて視聴を行うためのタイムシフト再生において、著作権侵害を回避することが可能な、記録装置、及び記録再生装置を提供することを目的とするものである。

上述した課題を解決するために、第１の発明（請求項１に対応）は、インターフェースから送られてくるデータを暗号化する暗号化手段と、

前記暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置である。

また、第２の発明（請求項２に対応）は、前記暗号化手段は、記録装置自らに割り付けられた固有の数値及び／または記号であるデバイスユニークキーを用いて、前記データを暗号化することを特徴とする第１の発明に記載の記録装置であ

る。

また、第３の発明（請求項３に対応）は、前記暗号化手段は、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記データを暗号化することを特徴とする第１または２の発明に記載の記録装置である。

また、第４の発明（請求項４に対応）は、前記記録ユニット情報を用いて、前記データを暗号化するとは、前記記録ユニット情報に基づいて得られたキーで前記データを暗号化することであることを特徴とする第３の発明に記載の記録装置である。

また、第５の発明（請求項５に対応）は、少なくとも前記記録ブロックに記録される前記暗号化されたデータ及び前記暗号化されたデータに付加された付加情報は、すべての部分が暗号化されて前記記録手段に記録されることを特徴とする第３または４の発明に記載の記録装置である。

また、第６の発明（請求項６に対応）は、前記データには、コピー許諾情報が付加されており、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第１の情報を作成し、

前記記録ユニット情報を用いて、前記暗号化手段は、前記第１の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする第３～５の発明のいずれかに記載の記録装置である。

また、第７の発明（請求項７に対応）は、前記データには、前記データに固有の数値及び／または記号であるタイトルキーが割り付けられており、

前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段に記録するように前記記録手段を制御することを特徴とする請求項２記載の記録装置。

また、第８の発明（請求項８に対応）は、前記暗号化手段は、前記タイトルキーを用いて前記データを暗号化することを特徴とする第７の発明に記載の記録装置である。

また、第９の発明（請求項９に対応）は、前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーを含む第３の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第３の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記

録手段を制御することを特徴とする第８の発明に記載の記録装置である。

また、第１０の発明（請求項１０に対応）は、前記データには、コピー許諾情報が付加されており、

前記暗号化手段は、前記コピー許諾情報をも用いて、前記データを暗号化することを特徴とする第８の発明に記載の記録装置である。

また、第１１の発明（請求項１１に対応）は、前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかを含む第２の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第２の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする第１０の発明に記載の記録装置である。

また、第１２の発明（請求項１２に対応）は、前記暗号化手段は、コピー許諾情報が付加され、インターフェースから送られてくるデータを前記コピー許諾情報を用いて暗号化し、

前記制御手段は、前記記録手段が前記データを記録する前及び／または前記データを記録した後に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第１の発明に記載の記録装置である。

また、第１３の発明（請求項１３に対応）は、前記制御手段は、少なくとも前記記録手段が前記データを記録する前に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第１２の発明に記載の記録装置である。

また、第１４の発明（請求項１４に対応）は、前記制御手段は、前記記録手段が前記データを記録した後のみに、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第１２の発明に記載の記録装置である。

また、第１５の発明（請求項１５に対応）は、インターフェースから送られてくる暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置である。

また、第１６の発明（請求項１６に対応）は、第１の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備えたことを特徴とする再生装置である。

また、第１７の発明（請求項１７に対応）は、第２の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記デバイスユニークキーを用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第１８の発明（請求項１８に対応）は、第３の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報を用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第１９の発明（請求項１９に対応）は、第４の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報に基づいて得られたキーで前記再生されたデータを復号することを特徴とする再生装置である。

また、第２０の発明（請求項２０に対応）は、第１４の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記データの記録時に、前記コピー許諾情報が前記記録手段に正常に記録出来

なかった場合、前記復号手段は、前記コピー許諾情報が各値を取ると仮定して前記暗号化されたデータの全部または一部の復号を試行し、

前記試行した結果、前記再生されたデータが正常に復号出来た場合の前記コピー許諾情報の値を用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第２１の発明（請求項２１に対応）は、第１５の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段とを備え、

前記再生されたデータは、インターフェースに送られることを特徴とする再生装置。

また、第２２の発明（請求項２２に対応）は、前記インターフェース、前記暗号化手段及び前記制御手段が、同一プリント基板上に一体化して配設されていることを特徴とする第１～１４の発明のいずれかに記載の記録装置である。

また、第２３の発明（請求項２３に対応）は、前記インターフェース、前記暗号化手段及び前記制御手段は、１チップ化されていることを特徴とする第２２の発明に記載の記録装置である。

また、第２４の発明（請求項２４に対応）は、前記インターフェース、前記復号手段及び前記制御手段が同一プリント基板上に一体化して配設されていることを特徴とする第１６～２０の発明のいずれかに記載の再生装置である。

また、第２５の発明（請求項２５に対応）は、前記インターフェース、前記復号手段及び前記制御手段は、１チップ化されていることを特徴とする第２４の発明に記載の再生装置である。

また、第２６の発明（請求項２６に対応）は、データとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする第２２の発明に記載の記録装置である。

また、第２７の発明（請求項２７に対応）は、第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする第２４の発明に記載の再生装置である。

また、第２８の発明（請求項２８に対応）は、第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする第２２の発明に記載の記録装置である。

また、第２９の発明（請求項２９に対応）は、第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする第２４の発明に記載の再生装置である。

また、第３０の発明（請求項３０に対応）は、前記デバイスユニークキーは、外部の機器がアクセスすることが出来ないことを特徴とする第２～１１の発明のいずれかに記載の記録装置である。

また、第３１の発明（請求項３１に対応）は、前記コピー許諾情報は、前記記録手段のユーザから直接アクセスできないシステム領域に記録されることを特徴とする第６、１０、１１、１２、１３、１４の発明のいずれかに記載の記録装置である。

また、第３２の発明（請求項３２に対応）は、前記インターフェースから送られてくるデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止（ｃｏｐｙ　ｎｅｖｅｒ）を表す場合であっても、前記記録手段が前記データを記録するように制御することが出来ることを特徴とする第１～１５、２２、２３、２６、２８、３０、３１の発明のいずれかに記載の記録装置である。

また、第３３の発明（請求項３３に対応）は、前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする第３２の発明に記載の記録装置である。

また、第３４の発明（請求項３４に対応）は、前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする第３２の発明に記載の記録装置である。

また、第３５の本発明（請求項３５に対応）は、前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止（ｃｏｐｙ　ｎｅｖｅｒ）を表す場合、前記再生手段が前記データを少なくとも１回再生するよう制御することを特徴とする第１６～２１、２４、２５、２７、２９の本発明のいずれかに記載の再生装置である。

また、第３６の発明（請求項３６に対応）は、前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする第３５の発明に記載の再生装置である。

また、第３７の発明（請求項３７に対応）は、前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする第３５の発明に記載の再生装置である。

また、第３８の発明（請求項３８に対応）は、前記記録された暗号化されたデ

ータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、１回だけ複製することを許可（ｃｏｐｙ　ｏｎｃｅ）することを表す場合、前記記録手段により１回複製された後の前記データの前記コピー許諾情報が、再び１回だけ複製することを許可（ｃｏｐｙ　ｏｎｃｅ）することを表すようにして、前記再生手段が前記データを１回だけ複製出力するよう制御することを特徴とする第１６～２１、２４、２５、２７、２９の発明のいずれかに記載の再生装置である。

また、第３９の発明（請求項３９に対応）は、前記所定の条件とは、前記再生手段が前記データを複製出力した所定の時間後に、前記データもしくは前記データの暗号化に用いたキーを消去する場合であるであることを特徴とする第３８の発明に記載の再生装置である。

また、第４０の発明（請求項４０に対応）は、前記所定の条件とは、１回だけ複製出力された前記データの記録先がバックアップ用として前記データを記録する装置である場合であることを特徴とする第３８の発明に記載の再生装置である。

また、第４１の発明（請求項４１に対応）は、前記記録先でバックアップ用として記録された前記データは、前記記録先では再生不可であることを特徴とする第４０の発明に記載の再生装置である。

また、第４２の発明（請求項４２に対応）は、前記記録先でバックアップ用として記録された前記データは、元の再生装置に戻さない限り再生不可であることを特徴とする第４０の発明に記載の再生装置である。

また、第４３の発明（請求項４３に対応）は、前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報の値に関係なく前記データ

を暗号化することを特徴とする第１～１４、２２、２３、２６、３０～３４の初ｓめいのいずれかに記載の記録装置である。

また、第４４の発明（請求項４４に対応）は、前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報が自由に複製してもよいこと（Ｃｏｐｙ　ｆｒｅｅ）を表す場合、前記データを暗号化せず、

前記制御手段は、前記記録手段が前記暗号化されていないデータを記録するように制御することを特徴とする第１～１４、２２、２３、２６、３０～３４の発明のいずれかに記載の記録装置である。

また、第４５の発明（請求項４５に対応）は、データが記録される記録媒体に記録されているデータを他の記録装置へ移動させる移動手段を少なくとも備えたデータ処理装置であって、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

ことを特徴とするデータ処理装置である。

また、第４６の発明（請求項４６に対応）は、データが記録される記録媒体に記録されているデータを他の記録装置に複写する複写手段を少なくとも備えたデータ処理装置であって、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

ことを特徴とするデータ処理装置である。

また、第４７の発明（請求項４７に対応）は、前記コピー禁止データを前記暗号化鍵で暗号化する暗号化手段をさらに備えたことを特徴とする第４５または４６の発明に記載のデータ処理装置である。

また、第４８の発明（請求項４８に対応）は、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する再生手段をさらに備えたことを特徴とする第４５～４７の発明のいずれかに記載のデータ処理装置である。

また、第４９の発明（請求項４９に対応）は、前記再生手段は、ユーザが視聴するさいに必要な速度で前記コピー禁止データを再生する手段であって、

前記他の記録装置から前記ユーザが視聴するさいに必要な速度よりも速い速度で、前記暗号化鍵で暗号化されている前記コピー禁止データが送信されてきた場合、送信されてきた前記コピー禁止データを、前記ユーザが視聴するさいに必要な速度よりも速い速度で格納する格納手段をさらに備え、

前記再生手段は、前記格納手段が前記他の記録装置からの前記コピー禁止データを格納するさいに、前記格納手段に格納された前記コピー禁止データもしくは、予め前記格納手段に格納されたデータを再生することができる

ことを特徴とする第４８の発明に記載のデータ処理装置である。

また、第５０の発明（請求項５０に対応）は、前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記第２の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第４５～４９の発明のいずれかに記載のデータ処理装置である。

また、第５１の発明（請求項５１に対応）は、前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第４５～４９の発明のいずれかに記載のデータ処理装置である。

また、第５２の発明（請求項５２に対応）は、前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを１回だけコピー可能なデータとして出力することを特徴とする第４５～５１の発明のいずれかに記載のデータ処理装置である。

また、第５３の発明（請求項５３に対応）は、第４５～４７の発明のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段を備えたことを特徴とする記録再生装置である。

また、第５４の発明（請求項５４に対応）は、第４８の発明に記載のデー

タ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置である。

また、第５５の発明（請求項５５に対応）は、第５０または５１の発明に記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置である。

また、第５６の発明（請求項５６に対応）は、第４５、４６、４７、５０、５１の発明のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する解読再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第５７の発明（請求項５７に対応）は、前記暗号化鍵が記録されている暗号化鍵記録媒体を再生する鍵再生手段と、

前記鍵再生手段が再生した前記暗号化鍵を記憶する鍵記憶手段とをさらに備え、

前記解読再生手段は、前記鍵記憶手段が記憶している前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする第５６の発明に記載の記録再生装置である。

また、第５８の発明（請求項５８に対応）は、前記データ処理装置から送信されてきた前記暗号化鍵を受信する受信手段をさらに備え、

前記解読再生手段は、前記受信手段によって受信された前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする第５６の発明に記載の記録再生装置である。

また、第５９の発明（請求項５９に対応）は、データが記録される記録媒体に記録されているデータを、他の記録装置へ、その他の記録装置において解読される形式のデータとして移動させる移動手段を少なくとも備え、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置である。

また、第６０の発明（請求項６０に対応）は、データが記録される記録媒体に記録されているデータを、他の記録装置に、その他の記録装置において解読される形式のデータとして複写する複写手段を少なくとも備え、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置である。

また、第６１の発明（請求項６１に対応）は、前記他の記録装置において

解読される形式のデータとは、平文データ、または前記他の記録装置固有の鍵で暗号化されたデータ、または前記他の記録装置における第２の記録媒体に付されている鍵で暗号化されたデータを意味することを特徴とする第５９または６０の発明に記載のデータ処理装置である。

また、第６２の発明（請求項６２に対応）は、前記他の記録装置において解読される形式のデータが、さらに、前記他の記録装置において用いられるフォーマットのデータでもあることを特徴とする第６１の発明に記載のデータ処理装置である。

また、第６３の発明（請求項６３に対応）は、前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記第２の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第５９～６２の発明のいずれかに記載のデータ処理装置である。

また、第６４の発明（請求項６４に対応）は、前記第２の記録媒体に、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であることを示す鍵が付されている場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第６３の発明に記載のデータ処理装置である。

また、第６５の発明（請求項６５に対応）は、前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第５９～６２の発明のいずれかに記載のデータ処理装置である。

また、第６６の発明（請求項６６に対応）は、前記他の記録装置が、前記データ処理装置に対応する装置であることを示す鍵を有している場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第６５の発明に記載のデータ処理装置である。

また、第６７の発明（請求項６７に対応）は、前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコ

ピー禁止データを１回だけコピー可能なデータとして出力することを特徴とする第５９～６６の発明のいずれかに記載のデータ処理装置である。

また、第６８の発明（請求項６８に対応）は、第５９または６０の発明に記載のデータ処理装置からの前記コピー禁止データを第２の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが平文データであり、

前記コピー禁止データを、前記第２の記録媒体に付されている暗号化鍵を用いて、または前記記録再生装置固有の暗号化鍵を用いて暗号化する暗号化手段と、

前記暗号化手段によって暗号化された前記コピー禁止データを前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第６９の発明（請求項６９に対応）は、第５９または６０の発明に記載のデータ処理装置からの前記コピー禁止データを第２の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが前記記録再生装置固有の鍵で暗号化されたデータ、または前記第２の記録媒体に付されている鍵で暗号化されたデータであり、

前記暗号化された前記コピー禁止データを前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化された前記コピー禁止デー

タを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第７０の発明（請求項７０に対応）は、前記移動手段が前記データの移動を行ったさい、または前記複写手段が前記データの複写を行ったさい、前記データの移動または複写に対する課金情報を、前記データ処理装置を管理する管理装置に送信する課金情報送信手段をさらに備えたことを特徴とする第４５、４６、４７、４８、４９、５０、５１、５２、５９、６０、６１、６２、６３、６４、６５、６６、６７の発明のいずれかに記載のデータ処理装置である。

また、第７１の発明（請求項７１に対応）は、前記データ処理装置と前記他の記録装置とが接続されたインタフェースに、少なくとも前記コピー禁止データの移動または複写に対して課金能力を有する管理装置が接続されていることが確認されたときに、前記移動手段または前記複写手段は、前記コピー禁止データを前記他の記録装置に移動させるまたは複写することを特徴とする第４５、４６、４７、４８、４９、５０、５１、５２、５９、６０、６１、６２、６３、６４、６５、６６、６７の発明のいずれかに記載のデータ処理装置である。

また、第７２の発明（請求項７２に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置と、

それら複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段

とを有する復号記録装置とを備えた

ことを特徴とする暗号化データ復号記録装置システムである。

また、第７３の発明（請求項７３に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、

前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを備えた

ことを特徴とする復号記録装置である。

また、第７４の発明（請求項７４に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置のうちの一つの記録装置であって、

前記暗号化された前記コピー禁止データを記録する記録手段と、その記録手段に記録されている前記暗号化されたコピー禁止データを出力する出力手段とを備え、

その出力手段から出力される前記暗号化されたコピー禁止データは、その暗号化されたコピー禁止データを復号する復号手段を少なくとも有する復号記録装置においてのみ復号されるデータである

ことを特徴とする記録装置である。

また、第７５の発明（請求項７５に対応）は、複数個のデータで構成されているストリームを送信する送信手段を備え、

前記ストリームの、または前記ストリームを構成する各ブロック内の、複数個の前記データそれぞれは、そのデータの時間上一つ手前のデータが再生

されないと再生されないデータであって、

前記送信手段は、前記ストリームの、または前記ストリームを構成する各ブロック内の、前記複数個のデータの時間的に最後尾から先頭側の順に、前記各データを送信する

ことを特徴とするデータ送信装置である。

また、第７６の発明（請求項７６に対応）は、複製が禁止または制限されるよう設定されているデータからなる複製制限コンテンツをタイムシフト再生可能にするための記録装置であって、

所定の容量分、前記複製制限コンテンツの記録が可能な記録媒体と、

前記記録媒体に対しデータの記録を行う記録手段とを備え、

前記記録手段は、前記複製制限コンテンツを前記記録媒体に記録するとともに、前記複製制限コンテンツの記録を開始した時刻から、所定の時間が経過した後、前記記録媒体に記録された前記複製制限コンテンツのデータを、視聴することが不可能な状態にすることを特徴とする記録装置である。

また、第７７の発明（請求項７７に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去することにより実現することを特徴とする第７６の発明に記載の記録装置である。

また、第７８の発明（請求項７８に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去しないことにより実現することを特徴とする第７６の発明に記載の記録装置である。

また、第７９の発明（請求項７９に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを再生不可能にすることにより実現することを特徴とする第７６の発明に記載の記録装置である。

また、第８０の発明（請求項８０に対応）は、前記視聴することが不可能な状態を、再生後の前記複製制限コンテンツのデータを暗号化することにより実現することを特徴とする第７９の発明に記載の記録装置である。

また、第８１の発明（請求項８１に対応）は、前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、前記複製制限コンテンツに関連した判別情報を参照することにより定められることを特徴とする第７６～８０の発明のいずれかに記載の記録装置である。

また、第８２の発明（請求項８２に対応）は、前記記録手段は、前記判別情報を用いて、前記複製制限コンテンツと他のコンテンツとを分別して記録を行うことを特徴とする第８１の発明に記載の記録装置である。

また、第８３の発明（請求項８３に対応）は、前記判別情報は、前記複製制限コンテンツのデータ列に含まれる著作権情報であることを特徴とする第８１の発明に記載の記録装置である。

また、第８４の発明（請求項８４に対応）は、前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、外部からの入力に基づき定められることを特徴とする第７６～８２の発明のいずれかに記載の記録装置である。

また、第８５の発明（請求項８５に対応）は、前記記録媒体は、前記複製制限コンテンツの一時記録を行うための記録バッファを有することを特徴とする第７６～８０の発明のいずれかに記載の記録装置である。

また、第８６の発明（請求項８６に対応）は、前記記録用バッファは、同一領域に上書き記録を繰り返すことにより一定量のデータを記録することが可能なリングバッファであることを特徴とする第８５の発明に記載の記録装

置である。

また、第８７の発明（請求項８７に対応）は、第７６～８５の発明のいずれかに記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置である。

また、第８８の発明（請求項８８に対応）は、第８６の発明に記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置である。

また、第８９の発明（請求項８９に対応）は、前記リングバッファに上書き記録が行われている状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上にて、最も古いデータが記録されている位置から該データの再生を行うことを特徴とする第８８の発明に記載の記録再生装置である。

また、第９０の発明（請求項９０に対応）は、前記リングバッファに上書き記録が行われていない状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上の記録開始位置から前記データの再生を行うことを特徴とする第８９の発明に記載の記録再生装置である。

また、第９１の発明（請求項９１に対応）は、前記記録装置は、前記記録媒体に記録された複製制限コンテンツが、前記所定の待機時間内に再生されない場合、該複製制限コンテンツの記録動作を停止することを特徴とする第８７または８８の発明に記載の記録再生装置である。

また、第９２の発明（請求項９２に対応）は、前記所定の時間または前記所定の待機時間のいずれかに基づき、前記記録装置または再生手段の動作内容をあらかじめ告知する告知手段をさらに備えたことを特徴とする第８７または８８の発明に記載の記録再生装置である。

また、第９３の発明（請求項９３に対応）は、前記記録手段は、前記所定の時間を含む時間情報を、計測できることを特徴とする第７６の発明に記載の記録装置である。

また、第９４の発明（請求項９４に対応）は、前記複製制限コンテンツは、前記所定の時間を含む時間情報を含んでいることを特徴とする第７６の発明に記載の記録装置である。

また、第９５の発明（請求項９５に対応）は、前記所定の時間を含む時間情報を、前記複製制限コンテンツとは独立して外部から取得することを特徴とする第７６の発明に記載の記録装置である。

また、第９６の発明は、第６の発明に記載の記録装置によってディスク記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、

前記復号手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第１の情報を作成し、

前記復号手段は、前記記録ユニット情報を用いて、前記第１の情報を復号した情報であるコンテンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置である。

また、第９７の発明は、第７の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、

前記復号手段は、前記暗号化されたタイトルキーを前記デバイスユニークキーを用いて復号することを特徴とする再生装置である。

また、第９８の発明は、第８の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記タイトルキーを用いて前記データを復号することを特徴とする再生装置である。

また、第９９の発明は、第９の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、

前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて復号し、

前記復号手段は、前記タイトルキーを含む第３の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手段は、前記第３の情報を復号した情報であるコンテンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置である。

また、第１００の発明は、第１０の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記コピー許諾情報を用いて前記データを復号することを特徴とする再生装置である。

また、第１０１の発明は、第１１の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するよ

うに前記記録手段を制御し、

前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて復号し、

前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、

前記復号手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかをを含む第２の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手段は、前記第２の情報を復号した情報であるコンテンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置である。

また、第１０２の発明は、第１２または１３の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記コピー許諾情報を再生するよう前記記録手段を制御し、

前記復号手段は、前記データを前記再生されたコピー許諾情報を用いて復号することを特徴とする再生装置である。

また、第１０３の発明は、第１～１０２のいずれかに記載の発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータ

により処理可能なことを特徴とする媒体である。

また、第１０４の発明は、第１～１０２のいずれかに記載の発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体である。

図面の簡単な説明

図１は、本発明の第１、２、４～６の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図２は、本発明の第１の実施の形態におけるハードディスク装置の機能概要を説明する図である。

図３は、本発明の第１の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図４は、本発明の第１の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図５は、（ａ）本発明の第１の実施の形態におけるハードディスク装置の記録時の動作を示すフローチャート図である。

（ｂ）本発明の第１の実施の形態におけるハードディスク装置の記録時の動作の連携を示す模式図である。

図６は、（ａ）本発明の第１の実施の形態におけるハードディスク装置の再生時の動作を示すフローチャート図である。

（ｂ）本発明の第１の実施の形態におけるハードディスク装置の再生時の動作の連携を示す模式図である。

図７は、（ａ）本発明の第１の実施の形態におけるハードディスク装置が用いる記録フォーマットを説明する図である。

（ｂ）上記（ａ）のフォーマットとは異なるフォーマットの例を示す図である。

図８は、ＣＣＩの値とその意味を説明する図である。

図９は、本発明の第１の実施の形態におけるハードディスク装置が記録再生する磁気ディスクのフォーマットを説明する図である。

図１０は、本発明の第３の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図１１は、本発明の第４の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図１２は、本発明の第４の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図１３は、本発明の第５の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図１４は、本発明の第５の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図１５は、本発明の第６の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図１６は、本発明の第６の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図１７は、（ａ）本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

（ｂ）本発明の実施の形態におけるハードディスク装置の復号手段の構成を示

すブロック図である。

図１８は、（ａ）本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

（ｂ）本発明の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図１９は、（ａ）本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

（ｂ）本発明の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図２０は、本発明の第７の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図２１は、本発明の実施の形態１のＡＶＨＤＤ１およびアーカイブ機器２のブロック図である。

図２２は、本発明の実施の形態１のＡＶＨＤＤ１２およびアーカイブ機器１３のブロック図である。

図２３は、本発明の実施の形態１のアーカイブ機器１６のブロック図である。

図２４は、本発明の実施の形態１のＡＶＨＤＤ１９およびアーカイブ機器２のブロック図である。

図２５は、本発明の実施の形態２のＡＶＨＤＤ２２およびアーカイブ機器２３のブロック図である。

図２６は、本発明の実施の形態４のＡＶＨＤＤ３２およびＤＶＤ装置３３のブロック図である。

図２７は、本発明の実施の形態４におけるストリームの構成図である。

図２８は、本発明の実施の形態１の、複写手段８０を備えたＡＶＨＤＤ８１のブロック図である。

図２９は、本発明の実施の形態２の、複写手段９０を備えたＡＶＨＤＤ９１のブロック図である。

図３０は、本発明の実施の形態３の暗号化データ復号記録システムのブロック図である。

図３１は、本発明の実施の形態３の記録装置１００のブロック図である。

図３２は、本発明の実施の形態３の復号記録装置１０１のブロック図である。

図３３は、本発明の実施の形態１による記録再生装置の構成図である。

図３４は、本発明の実施の形態１による記録再生装置の動作を説明するためのタイムチャートである。

図３５は、本発明の実施の形態１による記録再生装置の動作を説明するためのタイムチャートである。

図３６は、本発明の実施の形態２による記録再生装置の構成図である。

図３７は、本発明の実施の形態２による記録再生装置の動作を説明するためのタイムチャートである。

図３８は、本発明の実施の形態２による記録再生装置の動作を説明するためのタイムチャートである。

図３９は、本発明の実施の形態３による記録再生装置の動作を説明するためのタイムチャートである。

図４０は、本発明の実施の形態４による記録再生装置の構成図である。

図４１は、本発明の実施の形態５による記録再生装置の構成図である。

図４２は、本発明の実施の形態５による記録再生装置の動作を説明するための図である。

図４３は、従来の技術によるタイムシフト再生を行う記録再生装置の構成図である。

符号の説明

１　ＩＥＥＥ１３９４バス

２　ハードディスク装置

３　ホストシステム

４　Ｉ／Ｆ

１０　コントローラ

１１　暗号化手段

１２　復号手段

１３　デバイスユニークキー

１４　制御手段

１５　記録手段

１６　Ｉ／Ｆ

１７　暗号化されたコンテンツ

１８　秘密領域

１９　暗号器

２２　加算器

２３　タイトルキー

２４　ＣＣＩ

２５　記録ユニット番号

２６　コンテンツ

２７　ＣＣＩ

２８　暗号化されたタイトルキー

２９　磁気ディスク媒体

３１　復号器

３２　復号器

３３　復号器

３４　加算器

３５　タイトルキー

３６　ＣＣＩ

３７　復号されたコンテンツ

３９　記録ユニット

４１　フォーマット

４７　ハードディスク装置

５１　コントローラ

１００１、１０１２、１０１９、１０２２、１０３２　ＡＶＨＤＤ

１００２、１０１３、１０１６、１０２３　アーカイブ機器

１００３　ＳＴＢ

１００４、１０２８　暗号化手段

１００５　第１記録手段

１００６、１０２５、１０３４　蓄積手段

１００７、１０２７　移動手段

１００８、１０３１、１０３８　再生手段

１００９　第２記録手段

１０１０、１０２１　第２の記録媒体

１０１１、１０３５　送信手段

１０１４　バッファ

１０１５　高速送信手段

１０１７　解読再生手段

１０１８　ＩＣカード

１０２０　判断手段

１０２４　第３記録手段

１０２６　平文化手段

１０２９　第４記録手段

１０３０　第３の記録媒体

１０３３　ＤＶＤ装置

１０３６　第５記録手段

１０３７　ＤＶＤ

２０１０　判別情報検出手段

２０１１　時間情報取得手段

２０１２　記録再生手段

２０１３　記録媒体

２０１４　記録バッファ

２０１５　制御入力Ｉ／Ｆ

２０１６　切り替え手段

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

（第１の実施の形態）

まず、第１の実施の形態について説明する。

図１に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置２の構成を示す。

ハードディスク装置２は、ＩＥＥＥ１３９４バス１に接続され、さらにＩＥＥＥ１３９４バス１は、ホストシステム３に接続されている。

ＩＥＥＥ１３９４バス１は、ＡＶデータの転送やコマンドのやり取りを中継するＩＥＥＥ１３９４－１９９５に記述されているＩＥＥＥ　ｓｔａｎｄａｒｄ　ｆｏｒ　Ｈｉｇｈ　ｐｅｒｆｏｒｍａｎｃｅ　Ｓｅｒｉａｌ　Ｂｕｓである。

ホストシステム３は、ＩＥＥＥ１３９４インターフェースであるＩ／Ｆ１６を備えており、ハードディスク装置２に記録させるための著作権保護が必要なデータをＩＥＥＥ１３９４バス１に転送したり、ハードディスク装置２からの著作権保護が必要なデータをＩＥＥＥ１３９４バス１を介して受信して、再生する装置であり、例えばＳＴＢ（セットトップボックス：衛星放送受信器）などである。

ハードディスク装置２は、ＩＥＥＥ１３９４バス１を介してホストシステム３とＡＶデータをやり取りしながら、著作権を保護してＡＶデータを磁気ディスク媒体に記録及び／または磁気ディスク媒体から再生することが出来る装置である。

すなわち、ハードディスク装置２は、図２に示すように磁気ディスク媒体２９

に著作権保護が必要なＡＶデータを暗号化されたコンテンツ１７のように暗号化して記録し、また暗号化されたコンテンツ１７を再生する装置である。

ハードディスク装置２は、Ｉ／Ｆ４、コントローラ１０、記録手段１５から構成される。

また、コントローラ１０は、暗号化手段１１、復号手段１２、デバイスユニークキー１３、制御手段１４から構成される。

Ｉ／Ｆ４は、ＩＥＥＥ１３９４－ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）の方式のインターフェースであり、ＩＥＥＥ１３９４バス１を介して、ホストシステム３などの外部の機器とコマンドやＡＶデータをやりとりし、さらに、ＡＶデータを暗号化し、他の機器との認証を行い、認証が成功するか否かに応じて暗号を解読する鍵の無効化をするなどしてＩＥＥＥ１３９４バス１上に伝送されるＡＶデータの著作権を保護することが出来るインターフェースである。

コントローラ１０を構成する暗号化手段１１は、Ｉ／Ｆ４から送られてくるＡＶデータ及びＡＶデータに付加されたデータを暗号化する手段である。

復号手段１２は、記録手段１５が読み出したＡＶデータおよびＡＶデータに付加されたデータを復号する手段である。

暗号化手段１１と復号手段１２の構成は後述する。

デバイスユニークキー１３は、ハードディスク装置２の一台毎に固有に割り当てられた番号及び／または記号であり、ハードディスク装置２及び／またはコントローラ１０の外部からはアクセス出来ない領域に記録されているものである。

記録手段１５は、データを記録する磁気ディスク媒体、磁気ディスク媒体に対して情報の記録再生を行う磁気ヘッド、磁気ヘッドを先端に搭載し、磁気ディス

ク媒体の任意の半径位置に位置決め動作を行うアクチュエータ、磁気ディスク媒体を回転させるスピンドルモータなどから構成され、データを磁気ディスク媒体に書き込んだり磁気ディスク媒体からデータを読み出す手段である。記録手段１５がデータを読み書きする磁気ディスク媒体は、ハードディスク装置２に内蔵されており、ハードディスク装置２に対して着脱自在ではないものとする。

制御手段１４は、ＬＢＡを指定して、そのＬＢＡを記録手段１５の磁気ディスク媒体のヘッド、セクタに対応付け、アクチュエータ、スピンドルモータを制御して、磁気ヘッドを位置決めし、磁気ヘッドから磁気ディスク媒体に対してデータを書き込んだり読み込んだりするよう制御する手段である。

さて、前述したように図３に、暗号化手段１１の構成を示す。

暗号化手段１１は、暗号器１９、暗号器２０、暗号器２１、加算器２２から構成される。

また、図３で、デバイスユニークキー１３は、前述したようにハードディスク装置２に割り付けられたハードディスク装置２固有の数値及び／または記号である。すなわち、デバイスユニークキー１３はハードディスク装置２の一台毎に異なったものが割り当てられている。また、デバイスユニークキー１３は、ハードディスク装置２のコントローラ１０内に設けられた秘密領域１８に記憶されている。この秘密領域１８は、外部の機器が書き込みも読み出しもできないように保護された領域であり、コントローラ１０だけが秘密領域１８に記憶されている情報を読み出すことが出来る領域である。具体的には、この秘密領域１８は、プリント基板上のＲＯＭを用いて実現することが出来る。すなわち、デバイスユニークキー１３は、プリント基板上のＲＯＭに記録されている。つまり、このＲＯＭはハードディスク装置２及び／またはコントローラ１０の外部からはアクセス出

来ない。

タイトルキー２３は、ＡＶデータ毎に固有に割り付けられた数値及び／または記号である。

ＣＣＩ（Ｃｏｐｙ　ｃｏｎｔｒｏｌ　ｉｎｆｏｒｍａｔｉｏｎ）２４は、ＡＶデータに付加されており、コピー許諾情報を表す２ビットの数値であり、アイソクロナスパケットのアイソクロナスヘッダのｓｙ領域に付加されて送られてくるものである。

図８にＣＣＩの取り得る値とその意味を示す。ＣＣＩが１１の時、Ｃｏｐｙ　Ｎｅｖｅｒを意味する。すなわち、この値のＣＣＩが付加されているＡＶデータを視聴することが出来るが、そのＡＶデータをハードディスク装置２に記録するなどの複製を作成することを禁止する。

ＣＣＩが１０の時、Ｃｏｐｙ　Ｏｎｃｅを意味する。すなわち、この値のＣＣＩが付加されているＡＶデータを視聴することが出来、さらにハードディスク装置２に記録するなどそのＡＶデータの複製一世代だけ作成することが出来る。

ＣＣＩが０１の時、Ｎｏ　ｍｏｒｅ　Ｃｏｐｙを表す。すなわち、ＣＣＩがＣｏｐｙ　ＯｎｃｅであるＡＶデータを複製したＡＶデータはＮｏ　ｍｏｒｅ　Ｃｏｐｙとなる。すなわち、これ以上複製を作成することを禁止することを意味する。つまり、Ｎｏ　ｍｏｒｅ　Ｃｏｐｙは、Ｃｏｐｙ　Ｏｎｃｅのコンテンツを記録した後、再生時にこれ以上再コピーさせないようにするために必要である。

ＣＣＩが００の時、Ｃｏｐｙ　Ｆｒｅｅを意味する。すなわち、このＣＣＩの値が付加されているＡＶデータは自由に視聴することが出来、さらに　自由に複製を作成することが出来る。

記録ユニット番号２５は、制御手段１４が、記録手段１５に連続してアクセス

する最小単位である記録ユニットの大きさを持つ記録ブロックに固有の番号及び／または記号である。すなわち上記の異なった記録ブロックには異なった記録ユニット番号２５が割り当てられている。このような、記録ユニット番号２５は、ユーザや外部の機器には見えない秘密の情報である。記録ユニット番号２５と記録ユニットについては後述する。

なお、本実施の形態の記録ユニット番号２５は、本発明の記録ユニット情報の例である。

コンテンツ２６は、映画や音楽やドラマなどの番組を構成するＡＶデータである。

また、磁気ディスク媒体２９は、記録手段１５によってデータを読み書きされる磁気ディスクである。

暗号器１９は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込み、タイトルキー２３を暗号化して、暗号化されたタイトルキー２８を出力する手段である。

加算器２２は、タイトルキー２３の下位ビットに続けてＣＣＩ２４を付加した鍵生成用情報を生成する手段である。

なお、本実施の形態の鍵生成用情報は、本発明の第２の情報の例である。

暗号器２０は、鍵生成用情報を記録ユニット番号２５を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器２１は、コンテンツ２６をコンテンツキーを用いて暗号化する手段である。

また、図４に、復号手段１２の構成を示す。

復号手段１２は、復号器３１、復号器３２、復号器３３、加算器３４から構成

される。

また、図４で、デバイスユニークキー１３、タイトルキー３５、ＣＣＩ３６、記録ユニット番号２５、復号されたコンテンツ３７が図示されているが、これらは、それぞれ、図３で示したデバイスユニークキー１３、タイトルキー２３、ＣＣＩ２４、記録ユニット番号２５、コンテンツ２６に対応している。

また、磁気ディスク媒体２９は、記録手段１５によってデータを読み書きされる磁気ディスクであり、図３のものと同一である。

復号器３１は、秘密領域１８に記憶されいるデバイスユニークキー１３を読み込み、暗号化されたタイトルキー２８をデバイスユニークキー１３を用いて復号して、タイトルキー３５を出力する手段である。

加算器３４は、タイトルキー３５の下位ビットに続けてＣＣＩ２７を付加した鍵生成用情報を生成する手段である。

復号器３２は、鍵生成用情報を記録ユニット番号２５を用いて復号してコンテンツキーを生成する手段である。

復号器３３は、暗号化されたコンテンツ１７をコンテンツキーを用いて復号し、復号されたコンテンツ３７を出力する手段である。

図７の（ａ）に、記録手段１５の磁気ディスク媒体２９の記録フォーマットを示す。磁気ディスク媒体２９の領域は、記録ユニットのサイズの複数の記録ブロックである記録ユニット３９に分かれている。制御手段１４は、記録ユニット３９より小さい領域にはアクセス出来ず、また必ず３９などの記録ブロックの先頭からアクセスする。すなわち、制御手段１４は必ず記録ユニット３９の記録ブロック毎にデータを読み込みまたは書き込みを行う。

また、本実施の形態では、一つの記録ユニット３９をヘッダ３８とデータ４０

の領域に分けてＡＶデータを記録している。

データ４０は、トランスポートパケットが記録される領域である。またヘッダ３８には、暗号化されたタイトルキー３５が記録される。記録ユニット３９のヘッダ３８の領域に記録された情報も、データ４０の領域に記録された情報も全て暗号化されている。

すなわち、図７の（ｂ）に記録媒体の記録ブロックにＡＶデータを記録する別の例を示す。記録ブロック１５０をヘッダ１５１とデータ１５２に分けて記録するのは、本実施の形態の記録フォーマットと同一である。しかし、図７の（ｂ）ではヘッダ１５１の部分は非暗号化１５４の部分であり、データ１５５の部分は暗号化１５５の部分である。すなわち、データ１５２の部分のみ暗号化される。従って、ＩＥＥＥ１３９４バス１などを転送する際に暗号化して転送される鍵１５３がヘッダ１５１の部分に暗号化されずに記録されている。従ってヘッダ１５１の部分に外部の機器が不正にアクセスした場合、鍵１５３を外部の機器が入手することが出来るので、ＡＶデータの暗号が解読され、その著作権を保護することが出来ないことになる。

これに対して、本実施の形態の記録フォーマットは図７の（ａ）のように記録ユニット３９に記録されるデータを全て暗号化しているので、著作権を図７の（ｂ）のような記録フォーマットに較べてより確実に保護することが出来る。

このように、本実施の形態の記録フォーマットは、ハードディスク装置を製造するメーカに固有のものである。このため、標準的なフォーマットを採用している外部の機器からは、このようなメーカに固有のフォーマットで記録されているデータを読み取ることは困難である。従って、本実施の形態の記録フォーマットを用いることによって、磁気ディスク媒体２９に記録されているＡＶデータの著

作権を保護することが出来る。また、本実施の形態の記録フォーマットのセクタサイズや記録ユニットのサイズは自由に設計することが出来る。

記録ユニットの具体例としては、例えば磁気ディスク媒体２９のセクタがある。すなわち、１セクタ、連続する６２セクタ、連続する１２８セクタ、・・・・連続する２０４８セクタなど、連続する所定の個数のセクタを記録ユニット３９とすることが出来る。

また、前述した記録ユニット番号２５の具体例としては、例えばセクタのＬＢＡ（Ｌｏｇｉｃａｌ　ｂｌｏｃｋ　ａｄｒｅｓｓ）を記録ユニット番号２５とすることが出来る。すなわち、記録ユニット３９の先頭のセクタのＬＢＡ、記録ユニット３９の先頭から２番目のセクタのＬＢＡ、記録ユニット３９の先頭からＮ番目（Ｎは記録ユニットを構成するセクタの総数以下の整数）のいずれかを記録ユニット番号２５とすることが出来る。

あるいは、記録ユニット３９を一意に特定するための番号を使用することも出来る。すなわち、記録ユニット３９を磁気ディスク媒体２９の内周から外周に向かう順番に数えた場合の番号を記録ユニット番号２５とすることが出来る。

あるいは、記録ユニットを管理するために使用する内部管理用のアドレスを使用することも出来る。

あるいは、これらの複数通りの例を所定の規則に従って組み合わせて生成した数値や記号を用いてもよい。

要するに記録ユニット番号２５としては、ユーザからは見えない情報であり、磁気ディスク媒体２９の全ての記録ユニット３９を重複なく一意に特定する情報でありさえすればよい。

なお、本実施の形態のハードディスク装置２は本発明の記録装置の例であり、

本実施の形態のハードディスク装置２は本発明の再生装置の例でもあり、本実施の形態の記録手段は本発明の再生手段の例を兼ねている。

さらに、本実施の形態のＩ／Ｆ４は本発明のインターフェースの例であり、本実施の形態の磁気ディスク媒体２９は本発明のディスクの例である。

また、暗号化手段１１、復号手段１２及びデバイスユニークキー１３を含むコントローラ１３と、Ｉ／Ｆ４は一枚のプリント基板上に一体化して配設されている。また、暗号化手段１１、復号手段１２、制御手段１４、Ｉ／Ｆ４はそれぞれ１チップのＬＳＩとして実装されている。これらのチップの端子における信号は、公開されていないフォーマットに従ってビットの並べ替えなどのスクランブルが施されている。従って、これらの端子からＡＶデータとして再生出来る信号を外部の機器が取り出しても、信号を作成したフォーマットが解らないので、ＡＶデータとして再生することは容易でない。

次に、このような本実施の形態の動作を説明する。

まず、ハードディスク装置２が著作権保護を必要とするＡＶデータを記録する場合の動作を説明する。

なお、本実施の形態では、ＡＶデータは、ＭＰＥＧ２トランスポートストリーム形式で送られてくる。

図５の（ａ）にホストシステム３、ハードディスク装置２の主な動作をフローチャートで示す。以下、このフローチャートに従って説明する。また、図５の（ｂ）にホストシステム３、ハードディスク装置２の動作の連携を模式図を用いて示す。

ホストシステム３は、著作権保護を必要とするＡＶデータを暗号化し、アイソクロナスパケットとしてＩＥＥＥ１３９４バス１に伝送している。

Ｉ／Ｆ１６は、ＭＰＥＧ２トランスポートストリーム形式のＡＶデータを暗号化する。さらに、暗号化されたＭＰＥＧ２トランスポートストリームのトランスポートパケットにソースパケットヘッダを付加してソースパケットを作成する。そして、ソースパケットを分割または結合したデータブロックにＣＩＰヘッダを付加して、ＣＩＰを作成する。さらに、ＣＩＰにアイソクロナスヘッダを付加してアイソクロナスパケットを作成し、ＩＥＥＥ１３９４バス１に伝送する。

また、アイソクロナスパケットを生成する際に、図３のＣＣＩ２４は、アイソクロナスパケットのｓｙ領域に付加される。

ホストシステム３は、ハードディスク装置２にＡＶデータの記録を開始するコマンドを発行したとする。

このコマンドは、Ｉ／Ｆ１６からアシンクロナスパケットとして、ＩＥＥＥ１３９４バス１を経由してＩ／Ｆ４に送られる。

Ｉ／Ｆ４は記録開始を指示するコマンドを受信すると、Ｉ／Ｆ１６に認証を要求する。

これを受けてＩ／Ｆ１６とＩ／Ｆ４は認証動作を行う（Ｓ１）。図５の（ｂ）ではこの認証動作を認証８５で表した。

Ｉ／Ｆ１６は、ハードディスク装置２がＡＶデータを記録するのに適正な機器か不正な機器かを判断する。適正な機器であれば認証が成功し、不正な機器であれば認証が失敗する（Ｓ２）。

ハードディスク装置２がＡＶデータを記録する資格がない場合は、認証が失敗する（Ｓ３）。この場合ハードディスク装置２はＡＶデータを記録することが出来ない。

ハードディスク装置２がＡＶデータを記録することが出来る適正な機器である

場合、認証は成功する。

認証が成功すると、Ｉ／Ｆ４は、ホストシステム３が伝送しているアイソクロナスパケットをそのアイソクロナスチャンネルを識別して受信する。

そして、Ｉ／Ｆ４は、受信したアイソクロナスパケットのアイソクロナスヘッダからＣＣＩを分離する。

そして、ＣＣＩの値によって以下の動作を行う。

すなわち、図８において、ＣＣＩが１１の時、すなわちＣｏｐｙ　Ｎｅｖｅｒの場合、ＡＶデータを記録することが許可されていないので、Ｉ／Ｆ４は、記録処理をしないことをホストシステム３に通知し、コントローラ１０に記録処理を開始するよう指示しない。

ＣＣＩが１０の時、すなわち、Ｃｏｐｙ　Ｏｎｃｅの場合、Ｉ／Ｆ４は、記録処理を開始することをホストシステム３に通知し、さらにコントローラ１０に記録処理を開始するように指示する。

ＣＣＩが０１の時、すなわち、Ｎｏ　ｍｏｒｅ　Ｃｏｐｙの場合、Ｉ／Ｆ４は、ＣＣＩがＣｏｐｙ　Ｎｅｖｅｒと同様の動作を行う。

ＣＣＩが００の時、すなわち、Ｃｏｐｙ　Ｆｒｅｅの場合、記録処理を開始することをホストシステム３に通知し、さらにコントローラ１０に記録処理を開始するように指示する。

従って、ＣＣＩが１０の場合、Ｉ／Ｆ４は、認証動作の際にホストシステム３から受け取った鍵で暗号化されているＡＶデータを復号する。そして、復号したＡＶデータを、トランスポートパケット毎にソースパケットヘッダに付加されていた伝送用タイムスタンプの指示するタイミングで、トランスポートパケット毎に出力する。ＣＣＩが００の場合、ＡＶデータは暗号化されずに送られてくるの

で、復号処理をせず、伝送用タイムスタンプの指示するタイミングで、トランスポートパケット毎に出力する。

このように、Ｉ／Ｆ４から出力されるＡＶデータは復号され平文となっているが、ハードディスク装置２独自のフォーマットで記述された信号で出力されるので、第３者がＩ／Ｆ４のチップの端子から信号を取り出しても、第３者が利用出来るＡＶデータに復元することは非常に困難である。

暗号化手段１１は、Ｉ／Ｆ４から送られてくるＭＰＥＧ２トランスポートパケットを入力する。

まず、暗号器１９は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む（Ｓ４）。

暗号化手段１１は、Ｉ／Ｆ４から送られてきたＡＶデータに付加されているタイトルキー２３を検出する。そして、暗号器１９は、検出したタイトルキー２３をデバイスユニークキー１３によって暗号化する（Ｓ５）。

次に、暗号器１９が暗号化したタイトルキー２３は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９に暗号化されたタイトルキー２８のように記録される（Ｓ６）。この暗号化されたタイトルキー２８を、図５の（ｂ）にも示す。

さらに、暗号化手段１１は、ＡＶデータに付加されて送られてきたＣＣＩ２４を検出する。検出されたＣＣＩ２４は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９にＣＣＩ２７として記録される。

加算器２２は、タイトルキー２３の下位ビットに続けてＣＣＩ２４を付加した情報である鍵生成用情報を生成する。

一方、制御手段１４からＡＶデータの付加情報としてどの記録ユニットにＡＶ

データを記録するかの情報も送られてきている。暗号化手段１１は、記録する記録ユニットの記録ユニット番号２５を求める。

暗号器２０は、ＡＶデータを記録しようとしている記録ユニットの記録ユニット番号２５を用いて、加算器が生成した鍵生成用情報を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で暗号化したので、記録ユニット毎に変化する。

次に、暗号器２１は、これから記録するＡＶデータであるコンテンツ２６をコンテンツキーで暗号化する（Ｓ７）。

暗号化されたＡＶデータは、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９の記録すべき記録ユニットに暗号化されたコンテンツ１７として、記録される（Ｓ８）。図５の（ｂ）にも暗号化されたコンテンツ１７を示す。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号２５で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ２６を暗号化し（Ｓ７）、暗号化したコンテンツ１７を磁気ディスク媒体２９に記録する（Ｓ８）という動作を繰り返す。

このようにして、ハードディスク媒体２９は、著作権保護の必要なＡＶデータを磁気ディスク媒体２９に記録する。

次に、ハードディスク装置２が著作権保護を必要とするＡＶデータを再生する場合の動作を説明する。

図６の（ａ）にホストシステム３、ハードディスク装置２の再生時の主な動作をフローチャートで示す。以下、このフローチャートに従って説明する。また、図６の（ｂ）にホストシステム３、ハードディスク装置２の再生時の主な動作の

連携を説明する模式図を示す。

ホストシステム３がハードディスク装置２に再生開始を指示するコマンドを発行したとする。

このコマンドは、Ｉ／Ｆ１６からアシンクロナスパケットとして、ＩＥＥＥ１３９４バス１を経由してＩ／Ｆ４に送られる。

さらに、Ｉ／Ｆ１６は、Ｉ／Ｆ４に対して認証要求を行う。

これを受けてＩ／Ｆ１６とＩ／Ｆ４は認証動作を行う（Ｓ９）。この認証動作は、図６の（ｂ）では認証８６として示されている。

Ｉ／Ｆ４は、ホストシステム３がＡＶデータを利用するのに適正な機器が不正な機器かを判断する。適正な機器であれば認証が成功し、不正な機器であれば認証が失敗する（Ｓ１０）。

ホストシステム３がＡＶデータを利用する資格がない場合は、認証が失敗する（Ｓ１１）。この場合、ホストシステム３は、ＡＶデータを記録することが出来ない。

ホストシステム３がＡＶデータを記録することが出来る適正な機器である場合、認証は成功する。

認証が成功すると、Ｉ／Ｆ４は、ＡＶデータを再生するコマンドが送られてきたことをコントローラ１０に通知する。

復号手段１２は、この通知を受け取ると、まず、復号器３１は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む（Ｓ１２）。

さらに、制御手段１４の制御に従って、記録手段１５が暗号化されたタイトルキー２８を磁気ディスク媒体２９から読み出す（Ｓ１３）。図６の（ｂ）にも暗号化されたタイトルキー２８を示す。

復号器３１は、デバイスユニークキー１３によって、暗号化されたタイトルキー２８を復号する（Ｓ１４）。そして、復号手段１２は、復号されたタイトルキー３５をＩ／Ｆ４に転送する。

制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９からＣＣＩ２７を読み出す。

復号手段１２は、ＣＣＩ２７をＩ／Ｆ４に転送する。

加算器３４は、復号されたタイトルキー３５の下位ビットに続けて読み出したＣＣＩ２７を付加した情報である鍵生成情報を生成する。

制御手段１４は、読み取るべき記録ユニット３９を指定して、記録手段１５が記録ユニット３９に格納されている情報である暗号化されたコンテンツ１７を読み取るよう制御する。

復号手段１２は、記録ユニット３９の記録ユニット番号２５を求める。

復号器３２は、データを読み出そうとしている記録ユニット３９の記録ユニット番号２５を用いて、加算器が生成した鍵生成用情報を復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で復号したので、記録ユニット毎に変化する。

次に、制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ１７を読み出す（Ｓ１５）。図６の（ｂ）にも暗号化されたコンテンツ１７を示す。

次に、復号器３３は、記録手段１５が読み出した暗号化されたコンテンツ１７をコンテンツキーで復号する（Ｓ１６）。

復号手段１２は、復号されたコンテンツ３７をＩ／Ｆ４に転送する。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号２５で復号してコンテンツキーを生成し、暗号化されたコンテンツ１７を読み出し（Ｓ１５）、暗号化されたコンテンツ１７を、コンテンツキーで復号し（Ｓ１６）、復号したコンテンツ２７をＭＰＥＧ２トランスポートストリームとしてＩ／Ｆ４に転送するという動作を繰り返す。

また、復号手段１２から出力されるＡＶデータは復号されているが、ハードディスク装置２独自のフォーマットで記述された信号であるので、第３者が復号手段１２のチップの端子から信号を取り出しても、第３者が利用出来るＡＶデータに復元することは非常に困難である。

Ｉ／Ｆ４はコントローラ１０から送られきたＡＶデータを暗号化する。そして、アイソクロナスパケットとしてＩＥＥＥ１３９４バス１に転送する。

ホストシステム３のＩ／Ｆ１６は、アイソクロナスチャンネルを識別して、アイソクロナスパケットを受信し、暗号化されているＡＶデータを復号する。

Ｉ／Ｆ１６は、受信したＡＶデータをＭＰＥＧ２トランスポートストリームとして出力する。

出力されたＡＶデータはホストシステム３の有する図示していないトランスポートストリームデコーダで分離される。そして、図示していないＡＶデコーダがＡＶデコードしてアナログ信号に変換し、モニタに表示する。

このようにして、ハードディスク媒体２９は、著作権保護の必要なＡＶデータを磁気ディスク媒体２９から再生する。

本実施の形態のハードディスク装置２は、ＡＶデータの記録時、ＡＶデータの再生時、及び記録手段１５にＡＶデータが記録済みのいずれの場合でも、著作権保護が必要なＡＶデータの著作権を保護することが出来る。

なお、本実施の形態では、磁気ディスク２９がハードディスク装置２から着脱できないとして説明したが、これに限らず着脱自在であっても構わない。

さらに、本実施の形態では、デバイスユニークキー１３がハードディスク装置２のプリント基板上の秘密領域１８としてのＲＯＭに記憶されているとして説明したが、これに限らない。秘密領域１８を磁気ディスク媒体２９に設けても構わない。すなわち、デバイスユニークキー１３を磁気ディスク２９のユーザのアクセス出来ない領域に記憶しても構わない。

さらに、本実施の形態では、暗号化されたタイトルキー２８を磁気ディスク２９のユーザがアクセス出来るユーザ領域に記録するとして説明したが、これに限らない。ディスク媒体２９のユーザがアクセス出来ないシステム領域に記録しても構わない。また、ハードディスク装置２のプリント基板上に設けられたＲＡＭに記録しても構わない。

さらに、本発明の記録装置及び再生装置は、本実施の形態では、ハードディスク装置２として一体化されているとして説明したがこれに限らない。本発明の記録装置が、Ｉ／Ｆ４、暗号化手段１１、制御手段１４、記録手段１５から構成されており、ＡＶデータを記録する装置であり、また、本発明の再生装置が、Ｉ／Ｆ４、復号手段１２、制御手段１４、記録手段１５から構成されているなど、要するに本発明の記録装置は、暗号化手段と制御手段と記録手段を備えていさえすればよい。また、本発明の再生装置は、復号手段、制御手段を備えていさえすればよい。

さらに、本実施の形態のハードディスク装置２のＩ／Ｆ４、暗号化手段１１、復号手段１２、制御手段１４はそれぞれ１チップのＬＳＩで構成されているとして説明したが、これに限らない。Ｉ／Ｆ４、暗号化手段１１、復号手段１２、制

御手段１４がそれぞれ複数チップのＬＳＩから構成されていても構わない。また、チップの端子では、ＡＶデータは非公開のフォーマットで記述されているとして説明したがこれに限らず、端子間を伝送するために暗号化されていても構わない。また、チップの端子の性質が非公開のフォーマットで定められていても構わない。なお、ここでチップの端子の性質とは、どの端子がどのような信号を出力するか、またどの端子とどの端子とが組になってどのような信号を出力するか、また各端子がどのような用途に用いられるかなどの性質を表すものである。このようなチップの端子の性質が非公開のフォーマットで定められているため、例えば各端子がどのような用途に用いられるかなどをユーザが知ることが出来ないものである。要するに、Ｉ／Ｆ４、コントローラ１０が配設されているプリント基板上の端子及びチップの端子のうち、第３者がＡＶデータとして再生出来る信号を出力している端子で検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されているか、またはそれらの端子の性質が非公開のフォーマットで定められていさえすればよい。

さらに、本実施の形態のハードディスク装置２のＩ／Ｆ４、暗号化手段１１、復号手段１２、制御手段１４が１チップのＬＳＩで構成されていても構わない。このようにすればさらにＡＶデータの著作権を確実に保証することが出来る。

さらに、本実施の形態では、ＣＣＩを用いてＡＶデータを暗号化するとして説明したが、これに限らない。ＣＣＩを用いずにＡＶデータを暗号化しても構わない。すなわち、加算器２２が、ＣＣＩとタイトルキー２３から鍵生成用情報を作成する代わりに、加算器２２を用いず、タイトルキー２３を直接鍵生成用情報とし、この鍵生成用情報を記録ユニット番号で暗号化してコンテンツキーを生成しても構わない。なお、この場合のタイトルキー２３は本発明の第３の情報の例で

ある。このように、ＣＣＩを用いずにＡＶデータを暗号化する場合、本実施の形態のようにＣＣＩを磁気ディスク媒体２９に記録しても構わないし、また、ＣＣＩを磁気ディスク媒体２９に記録しなくても構わない。

さらに、本実施の形態では、ハードディスク装置２がＡＶデータに付加されているＣＣＩの値がＣｏｐｙ　ｎｅｖｅｒの場合、そのＡＶデータを記録せず、ＣＣＩの値がＣｏｐｙ　ｏｎｃｅの場合、そのＡＶデータを暗号化して記録し、ＣＣＩの値がＮｏ　ｍｏｒｅ　ｃｏｐｙの場合、そのＡＶデータを記録せず、ＣＣＩの値がＣｏｐｙ　ｆｒｅｅの場合、そのＡＶデータを暗号化して記録するとして説明したが、これに限らない。ＡＶデータに付加されているＣＣＩの値がいずれの値を取る場合であってもＡＶデータを暗号化して記録しても構わない。あるいは、ＡＶデータに付加されているＣＣＩの値がＣｏｐｙ　ｆｒｅｅの場合、そのＡＶデータを暗号化しないで平文のまま記録しても構わない。

さらに、本実施の形態では、鍵生成用情報は、復号されたタイトルキーの下位ビットに続けて読み出したＣＣＩを付加した情報であるとして説明したがこれに限らない。鍵生成用情報として、タイトルキーの上位ビットの前に読み出したＣＣＩを付加した情報であっても構わない。さらに、鍵生成用情報は、タイトルキーとＣＣＩのみを含む情報であっても構わないし、タイトルキーとＣＣＩを含み、さらにそれ以外の情報が含まれていても構わない。また、タイトルキーとＣＣＩのいずれか一方を含む情報であっても構わない。要するに本実施の形態の鍵生成用情報は、タイトルキーとＣＣＩの少なくともいずれかを含む情報でありさえすればよい。

（第２の実施の形態）

次に、第２の実施の形態について説明する。

本実施の形態では、ＣＣＩの処理を中心に説明する。

図１に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置２の構成を示す。

本実施の形態のハードディスク装置２の構成は第１の実施の形態と同一である。

図９に、記録手段１５の磁気ディスク媒体２９のフォーマット４１を示す。紙面左側が磁気ディスク媒体２９のディスク内周４５であり、紙面右側がディスク外周４６に対応している。ディスク内周４５側の領域は、システムＦＡＴ４２であり、ディスク外周４６側は、データ４３である。

システムＦＡＴ４２は、ユーザがアクセス出来ないシステム領域であり、ファイル管理情報など、制御手段１４がシステムを制御するために使用する領域である。

一方データ４３は、ユーザがアクセス出来る領域であり、ＡＶデータが記録されている。すなわち、図３、図４で示すような、暗号化されたコンテンツ１７、暗号化されたタイトルキー２８などが記録されている。

そして、ＣＣＩはＣＣＩデータ４４に示すようにシステムＦＡＴ４２にデータ４３を構成する記録ユニット毎に記録される。すなわち、記録ユニット毎にＣＣＩの値が割り付けられている。

また、ファイル管理情報とは、例えばＦＡＴ（ｆｉｌｅ　ａｌｌｏｃａｔｉｏｎ　Ｔａｂｌｅ）とディレクトリと呼ばれる情報からなる。

ＦＡＴは、記録ユニットのアドレスと次の記録ユニットのアドレスが対になったテーブルであり、ファイルのデータがどのような記録ユニットにどのような順番で格納されているかを示すものである。

また、ディレクトリは、ファイルを階層的に管理するテーブルであり、ファイ

ル名とファイルに格納されているデータが格納されている先頭の記録ユニットのアドレスと、ファイルが読み込み専用か、重ね書き可能かなどの属性を示す情報が対になったテーブルである。

ＦＡＴとディレクトリを用いれば、ファイルの作成、編集、消去などの処理を管理することが出来る。

次に、このような本実施の形態の動作を説明する。

第１の実施の形態と同様にしてハードディスク装置２は、ＡＶデータを記録している。このとき、ＡＶデータは第１の実施の形態と同様にして次々と記録ユニット毎に記録されていく。新しい記録ユニットにＡＶデータの記録が完了する毎に、ＡＶデータがどの記録ユニットに記録されたかを示すファイル管理情報を制御手段１４が作成、更新していく。そしてこのファイル管理情報を自らのメモリに保持していく。

そして、ＡＶデータの記録がすべて完了したタイミングで、制御手段１４は、作成、更新したファイル管理情報をシステムＦＡＴ４２に書き込み、システムＦＡＴ４２を最新のものに更新する。

最後に制御手段１４は、ＡＶデータが新規に書き込まれた記録ユニットのＣＣＩの値をファイル管理情報に書き込む。

このように、ＡＶデータを記録する際、まず、ＡＶデータが磁気ディスク媒体２９に記録され、ＡＶデータの記録が完了してから管理情報が磁気ディスク媒体２９に記録され、最後にＣＣＩがシステムＦＡＴ４２に書き込まれる。

ところで、ＡＶデータを記録中にユーザがハードディスク装置２の電源コンセントを誤って抜きとり、ハードディスク装置２の電源を切ってしまったとする。このような場合、すでに記録中であったＡＶデータのすでに記録された部分のフ

ァイル管理情報とＣＣＩは消えてしまう。

本実施の形態のハードディスク装置２は、このように記録が中断されたＡＶデータを次のようにして再生する。

制御手段１４は、磁気ディスク２９の空の記録ユニットに書き込む順番を所定の規則に従って決めている。

制御手段１４は、記録が中断されたＡＶデータをこの規則に従って記録されているとして、更新前のファイル管理情報から再生する。そして、暗号化手段１１は、ＣＣＩ２ビット分の値の組み合わせで復号を試みる。

そして、復号に成功したＣＣＩの値でさらに、最初からＡＶデータを復号する。

このように本実施の形態のハードディスク装置２は、記録が中断されたＡＶデータを正常に復号することが出来る。

さらに、ＡＶデータの終端は、トランスポートパケットに付加されているＰＣＲの値の連続性から検出する。

すなわち、ＰＣＲは、長くとも１００ｍｓの間隔でトランスポートパケットに付加されており、ＰＣＲの値は、２７ＭＨｚの周波数でカウントアップする上位３３ビット、下位９ビットのカウンタ値である。従って、ＰＣＲの値が１００ｍｓ以上に相当する値以上に変化すれば、ＡＶデータの終端を超えて別のＡＶデータを再生してしまったことがわかる。従って、暗号化手段１１は、ＰＣＲの値が連続である範囲のＡＶデータのみをＩ／Ｆ４に転送する。

なお、本実施の形態のハードディスク装置２は、第１の実施の形態と同様にして暗号化および復号を行うとして説明したがこれに限らない。第１の実施の形態とは別の暗号化を行っても構わない。要するにＣＣＩを用いて暗号化を行うハードディスク装置でありさえすればよい。

さらに本実施の形態のハードディスク装置２は、ＣＣＩの値を仮定して復号を試行するとして説明したがこれに限らない。ＡＶデータを記録する前にＣＣＩを磁気ディスク２９に記録し、ＡＶデータの記録が中断しても必ずＣＣＩが記録手段１５に記録されるようにしても構わない。

さらに、本発明の記録装置及び再生装置は、本実施の形態では、ハードディスク装置２として一体化されているとして説明したがこれに限らない。本発明の記録装置が、Ｉ／Ｆ４、暗号化手段１１、制御手段１４、記録手段１５から構成されており、ＡＶデータを記録する装置であり、また、本発明の再生装置が、Ｉ／Ｆ４、復号手段１２、制御手段１４、記録手段１５から構成されているなど、要するに本発明の記録装置は、暗号化手段と制御手段と記録手段を備えていさえすればよい。また、本発明の再生装置は、復号手段、制御手段を備えていさえすればよい。

さらに、本実施の形態では、ファイル管理情報は、ＦＡＴとディレクトリからなるとして説明したがこれに限らない。ＯＳ／２におけるＨＰＦＳ（ｈｉｇｈ ｐｅｒｆｏｒｍａｎｃｅ ｆｉｌｅ ｓｙｓｔｅｍ）、Ｍａｃ ＯＳのファイルシステム、ＵＮＩＸにおけるｉノード、Ｗｉｎｄｏｗｓ９５におけるＶＦＡＴ（ｖｉｒｔｕａｌ ＦＡＴ）、ＷｉｎｄｏｗｓＮＴのＮＴＦＳ（ｎｅｗ ｔｅｃｈｎｏｌｏｇｙ ｆｉｌｅ ｓｙｓｔｅｍ）などにおけるファイル管理情報を用いても構わない。ただし、その場合、第１の実施の形態で説明した記録ユニットを、これらのファイル管理情報の記録ブロックに一致させておく必要がある。要するにハードディスクに対して記録再生が可能なＯＳにおけるファイル管理情報を用いても構わない。

（第３の実施の形態）

次に、第３の実施の形態について説明する。

図１０に本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置４７の構成を示す。

本実施の形態のハードディスク装置４７は、第１の実施の形態のＩ／Ｆ４の代わりにＩ／Ｆ４８を備えている。また、本実施の形態のコントローラ５１は、暗号化手段１１、復号手段１２、デバイスユニークキー１３を持たない。

Ｉ／Ｆ４８は、ＩＥＥＥ１３９４バス１から送られてくる暗号化されたＡＶデータを復号せず、コントローラ５１に転送し、またコントローラ５１から送られてくる暗号化されたＡＶデータをそのままＩＥＥＥ１３９４バス１に転送するインターフェースである。それ以外は、第１の実施の形態のＩ／Ｆ４と同一である。

次に、このような本実施の形態のハードディスク装置４７の動作を第１の実施の形態との相違点を中心に説明する。

まず、ＡＶデータを記録する際の動作を説明する。

第１の実施の形態と同様にして、Ｉ／Ｆ１６とＩ／Ｆ４８が認証動作を行い、認証が成功したとする。そうすると、Ｉ／Ｆ４８はアイソクロナスチャンネルを識別してホストシステム３から送られてくるアイソクロナスパケットを受信する。

そして、アイソクロナスパケットからＭＰＥＧ２トランスポートストリームを復元する。そして、トランスポートパケットを順次コントローラ５１に転送する。

制御手段１４は、暗号化されているＡＶデータを記録手段１５が磁気ディスク２９に記録するように制御する。

それ以外は、第１の実施の形態と同一である。

このように本実施の形態のハードディスク装置４７は、暗号化されているＡＶデータをそのまま記録する。

次に、暗号化されているＡＶデータを再生する際の動作を説明する。

第１の実施の形態と同様にして、Ｉ／Ｆ１６とＩ／Ｆ４８が認証動作を行い、認証が成功したとする。そうすると、制御手段１４は、記録手段１５が暗号化されているＡＶデータを読み出すように制御する、そしてコントローラ５１は、読み出したＡＶデータをＭＰＥＧ２トランスポートストリームとしてＩ／Ｆ４８に転送する。

Ｉ／Ｆ４８は、暗号化されているＭＰＥＧ２トランスポートストリームをアイソクロナスパケットとしてＩＥＥＥ１３９４バス１に転送する。

それ以外は第１の実施の形態と同一である。

このように、本実施の形態のハードディスク装置４７は伝送用に暗号化されたＡＶデータをそのまま記録及び再生することによって簡易な構成で、ＡＶデータの著作権を保護することが出来る。

（第４の実施の形態）

次に、第４の実施の形態について説明する。

図１に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置２を示す。本実施の形態のハードディスク装置２は、第１の実施の形態で説明したハードディスク装置２の暗号化手段１１と復号手段１２の代わりに別の暗号化手段と復号手段に置き換えたものである。

図１１に本実施の形態のハードディスク装置２の暗号化手段６０を示す。また、図１２に本実施の形態の復号手段６１を示す。

本実施の形態では、第１の実施の形態との相違点である暗号化手段６０と復号手段６１を中心に説明する。

図１１において、暗号化手段６０は、暗号器１９、暗号器５２、暗号器２１か

ら構成される。すなわち、暗号化手段６０は、第１の実施の形態の暗号化手段１１とは異なり、ＣＣＩを用いて暗号化しない。

すなわち、暗号器１９は、秘密領域１８に記憶されいるデバイスユニークキー１３を読み込み、タイトルキー２３を暗号化して、暗号化されたタイトルキー２８を出力する手段である。

なお、本実施の形態のタイトルキー２３は、本発明の第１の情報の例である。

暗号器５２は、タイトルキー２３を記録ユニット番号２５を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器２１は、コンテンツ２６をコンテンツキーを用いて暗号化する手段である。

図１２に本実施の形態のハードディスク装置２の復号手段６１を示す。

図１２において、復号手段６１は、復号器３１、復号器５３、復号器３３から構成される。復号手段６１は、第１の実施の形態とは異なりＣＣＩを復号に用いない。

すなわち、復号器３１は、秘密領域１８に記憶されいるデバイスユニークキー１３を読み込み、暗号化されたタイトルキー２８をデバイスユニークキー１３を用いて復号して、タイトルキー３５を出力する手段である。

なお、本実施の形態のタイトルキー２８は本発明の第２の情報の例である。

復号器５３は、タイトルキー３５を記録ユニット番号２５を用いて復号してコンテンツキーを生成する手段である。

復号器３３は、暗号化されたコンテンツ１７をコンテンツキーを用いて復号し、復号されたコンテンツ３７を出力する手段である。

次に、このような本実施の形態の動作を第１の実施の形態との相違点である暗

号化手段６０と復号手段６１の動作を中心に説明する。

まず、暗号化手段６０の動作を説明する。

暗号器１９は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む。

暗号化手段６０は、Ｉ／Ｆ４から送られてきたＡＶデータに付加されているタイトルキー２３を検出する。そして、暗号器１９は、検出したタイトルキー２３をデバイスユニークキー１３によって暗号化する。

次に、暗号器１９が暗号化したタイトルキー２３は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９に暗号化されたタイトルキー２８のように記録される。

さらに、暗号化手段６０は、ＡＶデータに付加されて送られてきたＣＣＩ２４を検出する。検出されたＣＣＩ２４は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９にＣＣＩ２７として記録される。

暗号化手段６０は、記録する記録ユニットの記録ユニット番号２５を求める。

暗号器５２は、ＡＶデータを記録しようとしている記録ユニットの記録ユニット番号２５を用いて、タイトルキー２３を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で暗号化したので、記録ユニット毎に変化する。

次に、暗号器２１は、これから記録するＡＶデータであるコンテンツ２６をコンテンツキーで暗号化する。

暗号化されたＡＶデータは、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９の記録すべき記録ユニットに暗号化されたコンテンツ１７として、記録される。

以下、同様に、タイトルキー２３を、記録ユニット毎に、記録ユニット番号２５で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ２６を暗号化し、暗号化したコンテンツ１７を磁気ディスク媒体２９に記録するという動作を繰り返す。

このようにして、ハードディスク媒体２９は、著作権保護の必要なＡＶデータを磁気ディスク媒体２９に記録する。

次に、復号手段６１の動作を説明する。

復号器３１は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む。

さらに、制御手段１４の制御に従って、記録手段１５が暗号化されたタイトルキー２８を磁気ディスク媒体２９から読み出す。

復号器３１は、デバイスユニークキー１３によって、暗号化されたタイトルキー２８を復号する。そして、復号手段６１は、復号されたタイトルキー３５をＩ／Ｆ４に転送する。

制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９からＣＩ２７を読み出す。

復号手段１２は、ＣＣＩ２７をＩ／Ｆ４に転送する。

制御手段１４は、読み取るべき記録ユニット３９を指定して、記録手段１５が記録ユニット３９に格納されている情報である暗号化されたコンテンツ１７を読み取るよう制御する。

復号手段６１は、記録ユニット３９の記録ユニット番号２５を求める。

復号器５３は、データを読み出そうとしている記録ユニット３９の記録ユニット番号２５を用いて、タイトルキー３５を復号する。この復号した情報のことを

コンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で復号したので、記録ユニット毎に変化する。

次に、制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ１７を読み出す。

次に、復号器３３は、記録手段１５が読み出した暗号化されたコンテンツ１７をコンテンツキーで復号する。

復号手段６１は、復号されたコンテンツ３７をＩ／Ｆ４に転送する。

以下、同様に、タイトルキー３５を、記録ユニット毎に、記録ユニット番号２５で復号してコンテンツキーを生成し、暗号化されたコンテンツ１７を読み出し、暗号化されたコンテンツ１７を、コンテンツキーで復号し、復号したコンテンツ２７をＭＰＥＧ２トランスポートストリームとしてＩ／Ｆ４に転送するという動作を繰り返す。

本実施の形態で説明した暗号化手段６０と復号手段６１をハードディスク装置２に用いることにより、第１の実施の形態と同等の効果が得られる。

また、暗号化手段６０と復号手段６１を第１の実施の形態で説明した種々の変形例に適応出来ることは言うまでもない。

（第５の実施の形態）

次に、第５の実施の形態について説明する。

図１に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置２を示す。本実施の形態のハードディスク装置２は、第１の実施の形態で説明したハードディスク装置２の暗号化手段１１と復号手段１２の代わりに別の暗号化手段と復号手段に置き換えたものである。

図１３に本実施の形態のハードディスク装置２の暗号化手段６２を示す。また、図１４に本実施の形態の復号手段６３を示す。

本実施の形態では、第１の実施の形態との相違点である暗号化手段６２と復号手段６３を中心に説明する。

図１３において、暗号化手段６２は、加算器５４、暗号器５５、暗号器２１から構成される。本実施の形態の暗号化手段６２は、暗号化手段１１とは異なり、ＡＶデータの暗号化にタイトルキーを用いない。

すなわち、加算器５４は、デバイスユニークキー１３の下位ビットに続けてＣＣＩ２４を付加した鍵生成用情報を生成する手段である。

なお、本実施の形態の鍵生成用情報は本発明の第１の情報の例である。

暗号器５５は、鍵生成用情報を記録ユニット番号２５を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器２１は、コンテンツ２６をコンテンツキーを用いて暗号化する手段である。

図１４に本実施の形態のハードディスク装置２の復号手段６３を示す。

図１４において、復号手段１３は、加算器５６、復号器５７、復号器３３から構成される。

加算器５６は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込み、デバイスユニークキー１３の下位ビットに続けてＣＣＩ３６を付加した鍵生成用情報を生成する手段である。

復号器５７は、鍵生成用情報を記録ユニット番号２５を用いて復号してコンテンツキーを生成する手段である。

復号器３３は、暗号化されたコンテンツ１７をコンテンツキーを用いて復号し

、復号されたコンテンツ３７を出力する手段である。

次に、このような本実施の形態の動作を第１の実施の形態との相違点である暗号化手段６２と復号手段６３の動作を中心に説明する。

まず、暗号化手段６２の動作を説明する。

加算器５４は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む。そして、デバイスユニークキー１３の下位ビットに続けてＣＣＩ２４を付加した鍵生成用情報を生成する。

さらに、暗号化手段６２は、ＡＶデータに付加されて送られてきたＣＣＩ２４を検出する。検出されたＣＣＩ２４は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９にＣＣＩ２７として記録される。

そして、加算器５４は、デバイスユニークキー１３の下位ビットに続けてＣＣＩ２４を付加した鍵生成用情報を生成する。

暗号化手段６２は、記録する記録ユニットの記録ユニット番号２５を求める。

暗号器５５は、ＡＶデータを記録しようとしている記録ユニットの記録ユニット番号２５を用いて、鍵生成用情報を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で暗号化したので、記録ユニット毎に変化する。

次に、暗号器２１は、これから記録するＡＶデータであるコンテンツ２６をコンテンツキーで暗号化する。

暗号化されたＡＶデータは、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９の記録すべき記録ユニットに暗号化されたコンテンツ１７として、記録される。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号２５で

暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ２６を暗号化し、暗号化したコンテンツ１７を磁気ディスク媒体２９に記録するという動作を繰り返す。

このようにして、ハードディスク媒体２９は、著作権保護の必要なＡＶデータを磁気ディスク媒体２９に記録する。

次に、復号手段６３の動作を説明する。

加算器５６は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む。

制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９からＣＣＩ２７を読み出す。

復号手段６３は、ＣＣＩ２７をＩ／Ｆ４に転送する。

加算器５６は、デバイスユニークキー１３の下位ビットに続けてＣＣＩ２７を付加した鍵生成用情報を作成する。

制御手段１４は、読み取るべき記録ユニット３９を指定して、記録手段１５が記録ユニット３９に格納されている情報である暗号化されたコンテンツ１７を読み取りよう制御する。

復号手段６３は、記録ユニット３９の記録ユニット番号２５を求める。

復号器５７は、データを読み出そうとしている記録ユニット３９の記録ユニット番号２５を用いて、鍵生成用情報を復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で復号したので、記録ユニット毎に変化する。

次に、制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテン

ツ１７を読み出す。

次に、復号器３３は、記録手段１５が読み出した暗号化されたコンテンツ１７をコンテンツキーで復号する。

復号手段６３は、復号されたコンテンツ３７をＩ／Ｆ４に転送する。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号２５で復号してコンテンツキーを生成し、暗号化されたコンテンツ１７を読み出し、暗号化されたコンテンツ１７を、コンテンツキーで復号し、復号したコンテンツ２７をＭＰＥＧ２トランスポートストリームとしてＩ／Ｆ４に転送するという動作を繰り返す。

本実施の形態で説明した暗号化手段６２と復号手段６３をハードディスク装置２に用いることにより、第１の実施の形態と同等の効果が得られる。

また、暗号化手段６２と復号手段６３を第１の実施の形態で説明した種々の変形例に適応出来ることは言うまでもない。

（第６の実施の形態）

次に、第６の実施の形態について説明する。

図１に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置２を示す。本実施の形態のハードディスク装置２は、第１の実施の形態で説明したハードディスク装置２の暗号化手段１１と復号手段１２の代わりに別の暗号化手段と復号手段に置き換えたものである。

図１５に本実施の形態のハードディスク装置２の暗号化手段６４を示す。また、図１６に本実施の形態の復号手段６５を示す。

本実施の形態では、第１の実施の形態との相違点である暗号化手段６４と復号手段６５を中心に説明する。

図１５において、暗号化手段６４は、暗号器５８、暗号器２１から構成される。本実施の形態の暗号化手段６４は、暗号化手段１１とは異なり、ＡＶデータの暗号化にタイトルキーとＣＣＩを用いない。

すなわち、暗号器５８は、デバイスユニークキー１３を記録ユニット番号２５を用いて暗号化したものであるコンテンツキーを生成する手段である。

なお、本実施の形態のデバイスユニークキー１３は本発明の第１の情報の例である。

暗号器２１は、コンテンツ２６をコンテンツキーを用いて暗号化する手段である。

図１６に本実施の形態のハードディスク装置２の復号手段６５を示す。

図１６において、復号手段６５は、復号器５９、復号器３３から構成される。

復号器５９は、記録ユニット番号２５を用いてデバイスユニークキー１３を復号してコンテンツキーを生成する手段である。

復号器３３は、暗号化されたコンテンツ１７をコンテンツキーを用いて復号し、復号されたコンテンツ３７を出力する手段である。

次に、このような本実施の形態の動作を第１の実施の形態との相違点である暗号化手段６４と復号手段６５の動作を中心に説明する。

まず、暗号化手段６４の動作を説明する。

暗号化手段６４は、ＡＶデータに付加されて送られてきたＣＣＩ２４を検出する。検出されたＣＣＩ２４は、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９にＣＣＩ２７として記録される。

暗号器５８は、デバイスユニークキー１３を秘密領域１８から読み取る。

暗号化手段６４は、記録する記録ユニットの記録ユニット番号２５を求める。

暗号器５８は、ＡＶデータを記録しようとしている記録ユニットの記録ユニット番号２５を用いて、ディスクユニークキー１３を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で暗号化したので、記録ユニット毎に変化する。

次に、暗号器２１は、これから記録するＡＶデータであるコンテンツ２６をコンテンツキーで暗号化する。

暗号化されたＡＶデータは、制御手段１４の制御に従って、記録手段１５の磁気ディスク媒体２９の記録すべき記録ユニットに暗号化されたコンテンツ１７として、記録される。

以下、同様に、デバイスユニークキー１３を記録ユニット毎に、記録ユニット番号２５で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ２６を暗号化し、暗号化したコンテンツ１７を磁気ディスク媒体２９に記録するという動作を繰り返す。

このようにして、磁気ディスク媒体２９には、著作権保護の必要なＡＶデータが記録される。

次に、復号手段６３の動作を説明する。

復号器５９は、秘密領域１８に記憶されているデバイスユニークキー１３を読み込む。

制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９からＣＣＩ２７を読み出す。

復号手段６５は、ＣＣＩ２７をＩ／Ｆ４に転送する。

制御手段１４は、読み取るべき記録ユニット３９を指定して、記録手段１５が記録ユニット３９に格納されている情報である暗号化されたコンテンツ１７を読

み取りよう制御する。

復号手段６３は、記録ユニット３９の記録ユニット番号２５を求める。

復号器５９は、データを読み出そうとしている記録ユニット３９の記録ユニット番号２５を用いて、デバイスユニークキーを復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号２５で復号したので、記録ユニット毎に変化する。

次に、制御手段１４の制御に従って、記録手段１５は、磁気ディスク媒体２９の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ１７を読み出す。

次に、復号器３３は、記録手段１５が読み出した暗号化されたコンテンツ１７をコンテンツキーで復号する。

復号手段６３は、復号されたコンテンツ３７をＩ／Ｆ４に転送する。

以下、同様に、デバイスユニークキー１３を、記録ユニット毎に、記録ユニット番号２５で復号してコンテンツキーを生成し、暗号化されたコンテンツ１７を読み出し、暗号化されたコンテンツ１７を、コンテンツキーで復号し、復号したコンテンツ２７をＭＰＥＧ２トランスポートストリームとしてＩ／Ｆ４に転送するという動作を繰り返す。

このように、復号手段６５は、暗号化されたコンテンツ１７を復号する。

本実施の形態で説明した暗号化手段６４と復号手段６５をハードディスク装置２に用いることにより、第１の実施の形態と同等の効果が得られる。

また、暗号化手段６４と復号手段６５を第１の実施の形態で説明した種々の変形例に適応出来ることは言うまでもない。

なお、第４～６の実施の形態で、種々の暗号化手段と復号手段を示したが、こ

れに限らず、例えば図１７、図１８、図１９に示すようなものもハードディスク装置２の暗号化手段１１及び復号手段１２の代わりに用いることが出来る。

図１７の（ａ）に暗号化手段７３を示す。暗号化手段７３は、デバイスユニークキー１３を用いて暗号器６７がコンテンツ２６を暗号化するものである。

また、図１７の（ｂ）に復号手段７４を示す。復号手段７４は、暗号化手段７３によって暗号化されたコンテンツ１７を複合器６８がデバイスユニークキー１３を用いて復号し、復号されたコンテンツ３７を出力するものである。

図１８の（ａ）に、暗号化手段７５を示す。暗号化手段７５は、記録ユニット番号２５を用いて、暗号器６９がコンテンツ２６を暗号化するものである。

図１８の（ｂ）に、復号手段７６を示す。復号手段７６は、復号器７０が暗号化手段７５によって暗号化された暗号化されたコンテンツ１７を、記録ユニット番号２５を用いて復号し、復号されたコンテンツ３７を出力するものである。

図１９の（ａ）に、暗号化手段７７を示す。暗号化手段７７は、暗号器７１がデバイスユニークキー１３と記録ユニット番号２５を用いてコンテンツ２６を暗号化するものである。なお、暗号化手段７７に加算器を追加し、加算器がデバイスユニークキー１３と記録ユニット番号２５を結合し、その情報を用いて、暗号器７１がコンテンツ２６を暗号化する構成にすることもできる。

図１９の（ｂ）に、復号手段７８を示す。復号手段７８は、暗号化手段７７によって暗号化された暗号化されたコンテンツ１７を、復号器７２がデバイスユニークキー１３と記録ユニット番号２５を用いて復号するものである。

なお、復号手段７８に加算器を追加し、加算器がデバイスユニークキーと記録ユニット番号２５を結合し、その情報を用いて、復号器７２が暗号化されたコンテンツ１７を復号する構成でも構わない。

（第７の実施の形態）

次に、第７の実施の形態について説明する。

図２０の本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置８３の構成を示す。

ハードディスク装置８３は、第１の実施の形態のハードディスク装置２に加えてＣＣＩ判定手段７９、再生情報管理手段８０を備えている。また、第１の実施の形態のＩ／Ｆ４の代わりにＩ／Ｆ８１を、第１の実施の形態の制御手段１４の代わりに制御手段８２を備えている。

Ｉ／Ｆ８１の第１の実施の形態のＩ／Ｆ４との相違点は、ＩＥＥＥ１３９４バス１から受け取ったＡＶデータのＣＣＩがＣｏｐｙ　Ｎｅｖｅｒであっても、コントローラ１０に記録処理を開始するように通知し、コントローラ１０は、Ｉ／Ｆ８１からの通知に従って、ＡＶデータのＣＣＩがＣｏｐｙ　Ｎｅｖｅｒであっても所定の条件のもとではそのＡＶデータを記録することが出来る点である。

またＣＣＩ判定手段７９は、再生されたＡＶデータのＣＣＩの値を判定し、再生後のＣＣＩの値を決める手段である。

再生情報管理手段８０は、記録手段１５に記録されているＡＶデータを記録ユニット毎に一度再生されたかあるいは一度も再生されていないかの情報である再生情報を管理する手段である。

また、再生管理手段８０は、記録手段１５に記録されているＡＶデータが記録ユニット毎に他の機器に複製されたかまだ一度も複製されていないかを管理する手段でもある。

再生情報を参照すれば、記録ユニットに記録されているＡＶデータが１回再生済みであるかあるいは一度も再生されていないかを知ることが出来、例えば再生

情報は１ビットのフラグで表すことが出来る。

また、複製情報を参照すれば、記録ユニットに記録されているＡＶデータが１回複製されたかあるいはまだ一度も複製されていないかを知ることが出来る。

制御手段８２は、第１の実施の形態の制御手段１４に加えて、再生中のＡＶデータのＣＣＩをＣＣＩ判定手段７９に供給し、再生中のＡＶデータのＣＣＩと再生情報管理手段８０が生成更新している再生情報に従って、記録手段１５がＡＶデータの再生を行うか行わないかを制御し、また、他の機器への複製中のＡＶデータのＣＣＩをＣＣＩ判定手段７９に供給し、複製中のＡＶデータのＣＣＩと再生情報管理手段８０が生成更新している複製情報に従って、記録手段１５がＡＶデータの複製を行うか行わないかを制御する手段である。

なお、本実施の形態のＣＣＩ判定手段７９、制御手段８２、再生情報管理手段８０は、本発明の制御手段の例であり、本実施の形態のＩ／Ｆ８１は本発明のインターフェースの例である。

次に、このような本実施の形態の動作を第１の実施の形態との相違点を中心に説明する。

まず、記録時の動作を説明する。

ホストシステムからはＡＶデータが送られてきている。

Ｉ／Ｆ８１は、そのＡＶデータのＣＣＩがＣｏｐｙ　ｎｅｖｅｒの場合もコントローラ８４に記録を開始するように通知する。

暗号化手段１１は、ＡＶデータを暗号化する。

制御手段８２の制御に従って、記録手段１５は、暗号化されたＡＶデータを磁気ディスク２９に記録する。この際、第１の実施の形態と同様にＣＣＩも記録する。

ただし、制御手段８２は、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒの場合であっても、そのＡＶデータを記録する。しかし記録手段１５に記録されたＣＣＩがｃｏｐｙ　ｎｖｅｒのＡＶデータは、記録されてから所定の時間後に再生不可となる。どのようにして所定の時間後に再生不可となるかについては、後述する。

また、制御手段８２は、ＣＣＩがｃｏｐｙ　ｏｎｃｅのＡＶデータを複製するために出力するが、複製出力されてから所定の時間後には再生不可となる。これについても後述する。

再生情報管理手段８０は、記録ユニット毎にＡＶデータが記録手段１５に記録されると、再生情報と複製情報を次のように生成する。

すなわち、新規にＡＶデータが記録された時、記録ユニット毎に再生情報を未再生に設定し、複製情報を未複製に設定する。さらに、ＡＶデータが記録された時刻を記録する。

次に、このようにして記録されたＡＶデータを再生する場合の動作を説明する。

再生情報管理手段８０は、これから再生する記録ユニットのＡＶデータの再生情報を参照し、制御手段８２に通知する。

さらに、ＣＣＩ判定手段７９は、これから再生するＡＶデータのＣＣＩの値を判定し、再生出力される場合のＣＣＩの値を決定する。

すなわち、再生されたＡＶデータのＣＣＩがＣｏｐｙ　ｎｅｖｅｒの場合、Ｉ／Ｆ８１から出力する際のＣＣＩをＣｏｐｙ　ｎｅｖｅｒとする。また、再生されたＡＶデータのＣＣＩがＣｏｐｙ　ｏｎｃｅの場合、Ｉ／Ｆ８１から出力する際のＣＣＩをＮｏ　ｍｏｒｅ　ｃｏｐｙに変更する。また、ＣＣＩがＣｏｐｙ　ｆｒｅｅの場合、Ｉ／Ｆ８１から出力する際のＣＣＩをＣｏｐｙ　ｆｒｅｅとする。またＣＣＩの値がＮｏ　ｍｏｒｅ　ｃｏｐｙであるＡＶデータは記録されな

いので、ＣＣＩがＮｏ　ｍｏｒｅ　ｃｏｐｙとなることはない。

制御手段８２の制御に従って、記録手段がＡＶデータを再生する。

再生情報管理手段８０は、再生管理情報を次のように更新する。

すなわち、記録ユニット分のＡＶデータが再生されると、その再生情報を制御手段８２に通知する。また、記録ユニット分のＡＶデータが再生されるとその部分の再生情報を再生済みに設定する。

再生情報管理手段８０は、現在再生中のＡＶデータの再生情報がすでに再生済みであった場合、制御手段８２に通知する。

また、再生情報管理手段８０は、現在再生中のＡＶデータの時刻情報を制御手段８２に通知する。

制御手段８２は、ＣＣＩ判定手段７９によって変更される前のＣＣＩの値に応じて以下の動作をする。

すなわち、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータであれば、再生情報が再生済みの部分の再生を中止するように制御する。また、再生情報管理手段８０から通知された、そのＡＶデータに関する時刻情報が示す時刻から現在の時刻が所定の時間例えば２４０時間（１０日間）以上経過している場合、そのＡＶデータを再生しないよう制御する。

また、ＣＣＩがＣｏｐｙ　ｏｎｃｅのＡＶデータの場合は、再生情報の値に関わらず再生を継続するように制御する。

また、ＣＣＩがＣｏｐｙ　ｆｒｅｅのＡＶデータの場合は再生を継続するよう制御する。

このようにして再生されたＡＶデータは復号手段１２で復号される。

そして、Ｉ／Ｆ８１で伝送用に暗号化されてＩＥＥＥ１３９４バス１にアイソ

クロナスパケットとして出力される。この際アイソクロナスヘッダには、上記のようにＣＣＩ判定手段７９が決めたＣＣＩが付加されている。

次に、このようにして記録されたＡＶデータを複製する場合の動作を説明する。

再生情報管理手段８０は、これから複製する記録ユニットのＡＶデータの複製情報を参照し、制御手段８２に通知する。

さらに、ＣＣＩ判定手段７９は、これから複製するＡＶデータのＣＣＩの値を判定し、再生出力される場合のＣＣＩの値を決定する。

すなわち、再生されたＡＶデータのＣＣＩがＣｏｐｙ　ｎｅｖｅｒの場合、Ｉ／Ｆ８１から出力する際のＣＣＩを設定しないかまたはＣｏｐｙ　ｎｅｖｅｒとする。また、再生されたＡＶデータのＣＣＩがＣｏｐｙ　ｏｎｃｅの場合、Ｉ／Ｆ８１から出力する際のＣＣＩをＣｏｐｙ　ｏｎｃｅのままにし、Ｎｏ　ｍｏｒｅ　ｃｏｐｙに変更しない。また、ＣＣＩがＣｏｐｙ　ｆｒｅｅの場合、Ｉ／Ｆ８１から出力する際のＣＣＩをＣｏｐｙ　ｆｒｅｅとする。またＣＣＩの値がＮｏ　ｍｏｒｅ　ｃｏｐｙであるＡＶデータは記録されないので、ＣＣＩがＮｏ　ｍｏｒｅ　ｃｏｐｙとなることは、ない。

制御手段８２の制御に従って、記録手段が複製されるＡＶデータを再生する。

再生情報管理手段８０は、複製管理情報を次のように更新する。

すなわち、記録ユニット分のＡＶデータが複製されると、その複製情報を制御手段８２に通知する。また、記録ユニット分のＡＶデータが複製されるとその部分の複製情報を複製済みに設定する。

再生情報管理手段８０は、現在複製中のＡＶデータの複製情報がすでに複製済みであった場合、制御手段８２に通知する。

制御手段８２は、ＣＣＩ判定手段７９によって変更される前のＣＣＩの値に応

じて以下の動作をする。

すなわち、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータであれば、複製をおこなわないように制御する。

また、ＣＣＩがＣｏｐｙ　ｏｎｃｅのＡＶデータの場合は、複製情報が複製済みの部分の複製を行わないよう制御し、複製情報が未複製の場合は、その部分のＡＶデータの記録先の装置がバックアップ用として前記データを記録する装置である場合に限り、複製を継続するよう制御する。

また、ＣＣＩがＣｏｐｙ　ｆｒｅｅのＡＶデータの場合は複製を継続するよう制御する。

このようにして複製されるために再生されたＡＶデータは復号手段１２で復号される。

そして、Ｉ／Ｆ８１で伝送用に暗号化されてＩＥＥＥ１３９４バス１にアイソクロナスパケットとして出力される。この際アイソクロナスヘッダには、上記のようにＣＣＩ判定手段７９が決めたＣＣＩが付加されている。ＩＥＥＥ１３９４バス１を経由して他の機器で受信されて、記録される。

また、複製されたＡＶデータのＣＣＩがｃｏｐｙ　ｏｎｃｅの場合、バックアップ用として記録された記録先ではそのＡＶデータを再生することが出来ず、元のハードディスク８３に戻さないと再生出来ない。

すなわち、本実施の形態のハードディスク装置８３は、Ｃｏｐｙ　ｎｅｖｅｒのＡＶデータを記録し、一回だけ再生することが出来る。

ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータは記録することが許されていないので、放送される時間帯にのみ視聴するものであった。

しかし、本実施の形態のハードディスク装置８３を用いれば、著作権者の意図

を守ったまま、ＡＶデータを放送される時間帯とは別の時間帯に視聴することが出来る。

また、ＣＣＩがＣｏｐｙ　ｏｎｃｅのＡＶデータは一回だけコピーすることが許可されるものであった。すなわち、一度、Ｃｏｐｙ　ｏｎｃｅのＡＶデータを記録すると、記録した装置からそのＡＶデータを再生することしか出来なかった。

しかし、本実施の形態のハードディスク装置８３を用いれば、Ｃｏｐｙ　ｏｎｃｅのＡＶデータを Ｃｏｐｙ　ｏｎｃｅのＣＣＩのまま一回だけ複製することが出来るので、著作権の意図するところを守ったままそのＡＶデータを別の記録再生装置に移動することが出来る。

なお、本実施の形態では、再生情報管理手段８０が、記録ユニット分のＡＶデータが再生されると、その再生情報を制御手段８２に通知し、記録ユニット分のＡＶデータが再生されるとその部分の再生情報を再生済みに設定することにより、本実施の形態のハードディスク装置８３は、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータを１回だけ再生することが出来るとして説明したが、これに限らない。再生情報管理手段８０が再生情報を更新する方法を以下のようにしても構わない。

すなわち、再生情報管理手段８０が、記録ユニット分のＡＶデータが何回再生されたかをカウントし、所定の回数例えば５回だけ再生されてはじめてその記録ユニット分のＡＶデータの再生情報を再生済みに設定しても構わない。このようにすれば、ハードディスク装置８３は、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータを所定の回数だけ再生することが出来るようになる。

また、再生情報管理手段８０が、一つのＡＶデータのうちの各記録ユニットに記録されている部分が再生されたか回数をカウントし、一つのＡＶデータの全て

の記録ユニットに記録されている部分が全て再生された時点で、再生情報管理手段８０がこの一つのＡＶデータの全ての記録ユニットに記録されている部分の再生管理情報を再生済みに設定しても構わない。このようにすれば、ハードディスク装置８３は、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータの一部を何回でも再生することが出来るようになり、そのＡＶデータの全部が再生された時点ではじめて再生不可になる。

さらに、本実施の形態では、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータは記録されてから所定の時間が経過すると再生不可となるとして説明したが、これに限らず、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータが課金条件によって再生不可とっても構わない。このような課金条件としては、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒのＡＶデータを記録したときに所定の代金の支払い手続きを行った場合には再生可として、その支払い手津付きを行わなかった場合には再生不可となるなどの条件がある。

さらに、本実施の形態では、ＣＣＩがｃｏｐｙ　ｏｎｃｅのＡＶデータは、複製情報が未複製の場合は、その部分のＡＶデータの記録先の装置がバックアップ用として前記データを記録する装置である場合に限り、複製を継続するよう制御するとして説明したが、これに限らず、ＣＣＩがｃｏｐｙ　ｏｎｃｅのＡＶデータを記録してから所定の時間が経過するとその記録されたＡＶデータまたはそのデータを記録する際の暗号化に用いたキーを消去しても構わない。

このように、本実施の形態のハードディスク装置８３は、ＣＣＩがｃｏｐｙ　ｎｅｖｅｒのＡＶデータを記録したり、ＣＣＩがＣｏｐｙ　ｏｎｃｅのＡＶデータをＣｏｐｙ　ｏｎｃｅのＣＣＩのまま一回だけ再生したりするので、

著作権者の意図するところを守っているとは言え、著作権違反をしているとも捉えることが出来る。すなわち、ＣＣＩがｃｏｐｙ　ｎｅｖｅｒである場合には、絶対複製をしてはいけないという意味があるからである。ところで、このようなＣＣＩの意味を拡張した拡張ＣＣＩの使用が現在検討中である。拡張ＣＣＩではｃｏｐｙ　ｎｅｖｅｒやｃｏｐｙ　ｏｎｃｅの意味を拡張して解釈される。本実施の形態のハードディスク装置８３は、このような従来のＣＣＩの代わりに拡張ＣＣＩを用いて上記のような動作を行うことも出来る。このように本実施の形態のハードディスク装置８３が拡張ＣＣＩを用いて上記のような動作を行えば、著作権違反を犯していることにはならなくなる。

このように、本実施の形態のハードディスク装置８３を用いれば、記録することが許されていないＡＶデータが放送される時間帯以外の任意の時間に視聴することが出来る。また、１世代しか複製を作ることが許されていないＡＶデータを別の記録装置に移動することが出来るのでバックアップ装置としても使用することが出来る。

なお、記録することが許されていないＡＶデータを放送される時間帯以外の任意の時間帯に視聴したり、バックアップすることについては、以下の実施の形態でさらに、詳細に説明する。

なお、本実施の形態のハードディスク装置８３にも、第１の実施の形態で説明した種々の変形が可能であることは言うまでもない。

さらに、本実施の形態のハードディスク装置８３は、暗号化手段１１、復号手段１２を備えているとして説明したが、第１の実施の形態以降で説明した暗号化手段、復号手段を用いても構わない。

さらに、本発明のデータは、本実施の形態におけるＡＶデータに限らない。イ

ンターネットなどから送られてくる文書データや画像データ、インターネットなどから送られてくるゲームソフトや文書作成ソフトなどのコンピュータプログラムであっても構わない。要するに本発明のデータとは、本発明のディスクに記録し、本発明のディスクから再生して利用することが出来るものでありさえすればよい。

さらに、本発明のインターフェースは、本実施の形態におけるＩＥＥＥ１３９４インターフェースに限らず、ＵＳＢのインターフェースであっても構わない。

さらに、本発明のディスクは、本実施の形態における磁気ディスク媒体に限らず、光ディスク媒体や光磁気ディスク媒体などであっても構わない。要するに本発明のディスクは、記録時及び／または再生時にデータにランダムアクセスすることが出来る記録媒体でありさえすればよい。

さらに、本発明のコピー許諾情報は、本実施の形態におけるＣＣＩや拡張ＣＣＩなどに限らず、要するにデータを複製することに関する許諾を示す情報でありさえすればよい。

なお、以上の実施の形態では、ＡＶデータに付加されているＣＣＩの値として、Ｃｏｐｙ　ｎｅｖｅｒ、Ｃｏｐｙ　ｏｎｃｅ、Ｎｏ　ｍｏｒｅ　ｃｏｐｙ、Ｃｏｐｙ　ｆｒｅｅがあるとして説明したが、以下に説明する第８～第１１の実施の形態では、ＣＣＩの値がＣｏｐｙ　Ｎｅｖｅｒ、Ｃｏｐｙ　ｏｎｃｅ、及びＮｏ　ｍｏｒｅ　ＣｏｐｙのいずれかであるＡＶデータは、コピー禁止データとして一括して扱うものとする。また、コピー禁止データのＣＣＩが上記のＣｏｐｙ　Ｎｅｖｅｒ、Ｃｏｐｙ　ｏｎｃｅ、及びＮｏ　ｍｏｒｅ　Ｃｏｐｙのいずれに対応しているかについては、第８～第１１の実施の形態で個別に説明するものとする。

（第８の実施の形態）

次に、本発明の第８の実施の形態のＡＶＨＤＤ１００１およびアーカイブ機器１００２の構成を述べる。

図２１に、本発明の第８の実施の形態のＡＶＨＤＤ１００１およびアーカイブ機器１００２のブロック図を示す。なお、図２１には説明の便宜上、ＳＴＢ（セットトップボックス）１００３をも表示している。

さて、本発明の第８の実施の形態のＡＶＨＤＤ１００１は、図２１に示すように、ＳＴＢ１００３からのデータをＡＶＨＤＤ１００１固有の暗号化鍵で暗号化する暗号化手段１００４と、暗号化手段１００４によって暗号化されたデータを蓄積手段１００６内の記録媒体に記録する第１記録手段１００５と、データを蓄積する蓄積手段１００６と、蓄積手段１００６に蓄積されているデータをアーカイブ機器１００２に移動させる移動手段１００７と、アーカイブ機器１００２からのデータであって、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読し再生する再生手段８とで構成されている。なお、蓄積手段１００６は、データが記録される第１の記録媒体を有しており、データはその第１の記録媒体に記録される。

なお「発明の実施の形態」では、ＡＶＨＤＤを、ハードディスクドライブ（ＨＤＤ）を用いて、音声（Ａｕｄｉｏ）や映像（Ｖｉｄｅｏ）やその他のデータを記録再生する装置を表す単語として用いる。

次に、本発明の第８の実施の形態のアーカイブ機器１００２は、図２１に示すように、ＡＶＨＤＤ１００１からのデータを第２の記録媒体１０１０に記録する第２記録手段１００９と、第２の記録媒体１０１０と、第２の記録媒体１０１０に記録されているデータを読み出してＡＶＨＤＤ１００１に送

信する送信手段１０１１とで構成されている。なお、アーカイブ機器１００２としては、例えばＤＶＤ装置や、Ｄ－ＶＨＳ装置が該当する。本実施の形態では、アーカイブ機器１００２の一例としてＤＶＤ装置を用いて説明することにする。したがって、第２の記録媒体１０１０の一例としてはＤＶＤが該当することになる。

なお、ＳＴＢ１００３は、例えば放送局からのデータを受信し、そのデータをＡＶＨＤＤ１００１に出力するとともに、ＡＶＨＤＤ１００１からのデータを再生する手段であって、再生されたデータは、映像データであればＳＴＢ１００３に接続されているディスプレイに表示され、また音声データであればＳＴＢ１００３に接続されているスピーカから出力される。なお、ディスプレイやスピーカは図示されていない。

また、第８の実施の形態では、本発明の、データ処理装置の一例としてＡＶＨＤＤ１００１を、記録再生装置の一例としてアーカイブ機器１００２を、それぞれ用いる。

また、ＡＶＨＤＤ１００１の蓄積手段１００６内の第１の記録媒体は、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。同様に、アーカイブ機器１００２内の第２の記録媒体１０１０も、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。

また、ＡＶＨＤＤ１００１とアーカイブ機器１００２との接続は、ＩＥＥＥ１３９４規格のインターフェースを介して行われていてもよいし、ＩＤＥ規格のインターフェースを介して行われていてもよい。または、他のインターフェースを介して行われていてもよい。ＡＶＨＤＤ１００１とＳＴＢ１０

０３との接続についても、いずれのインターフェースを介して行われていてもよい。

次に、本発明の第８の実施の形態のＡＶＨＤＤ１００１およびアーカイブ機器１００２の動作を述べる。

以下の説明の便宜上、ＡＶＨＤＤ１００１の蓄積手段１００６内の第１の記録媒体の記録可能容量が限界に達しようとしており、いずれかのデータを上書きまたは削除しなければＳＴＢ１００３からの新たなデータを蓄積することができない状態であるとし、ユーザが、蓄積手段１００６内のデータをアーカイブ機器１００２内の第２の記録媒体１０１０に移動させるための指示を、ＡＶＨＤＤ１００１およびアーカイブ機器１００２にしたものとする。

なお、データの移動とは、例えば第１の記録媒体に記録されているデータを、別の第２の記録媒体に移し、移した後には第１の記録媒体内には移ったデータを残さないことを意味する。

また、以下の説明の便宜上、ＡＶＨＤＤ１００１からアーカイブ機器１００２に移動させられるデータは、暗号化手段１００４によってＡＶＨＤＤ１００１固有の暗号化鍵で暗号化され、第１記録手段１００５によって蓄積手段１００６内の第１の記録媒体に記録されていたものとする。また、上記の移動対象のデータは、著作権保護のために、他の記録装置への移動は許されているがコピーが禁止されているコピー禁止データであるとする。

さてこのとき、移動手段１００７は、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているコピー禁止データを、蓄積手段１００６内の第１の記録媒体から読み出してアーカイブ機器１００２に送信する。このようにして移動手段１００７がコピー禁止データを送信するさい（移動させるさい）、そ

の移動手段１００７は、コピー禁止データを１回だけコピー可能なデータとして出力する。

そして、アーカイブ機器１００２では、第２記録手段１００９が、ＡＶＨＤＤ１００１からのコピー禁止データを第２の記録媒体１０１０に記録する。なお、移動手段１００７によってアーカイブ機器１００２に移動させられるデータは、ＡＶＨＤＤ１００１内において復号されずに暗号化されたままアーカイブ機器１００２に移動させられる。したがって、第２記録手段１００９によって第２の記録媒体１０１０に記録されたデータは、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているコピー禁止データであるということになる。

次に、第２の記録媒体１０１０に記録された、暗号化されているコピー禁止データを再生する場合について説明する。図２１に示すように、アーカイブ機器１００２には、暗号化されたコピー禁止データを解読し再生する手段が設けられていないので、コピー禁止データを解読し再生することができる、ＡＶＨＤＤ１００１の再生手段１００８に再度データを移動させる必要がある。

そこで、第２の記録媒体１０１０に記録された、暗号化されているコピー禁止データを再生する場合には、送信手段１０１１が、第２の記録媒体１０１０に記録されているデータを読み出してＡＶＨＤＤ１００１に送信し、ＡＶＨＤＤ１００１において、再生手段１００８が、暗号化されたコピー禁止データを解読し再生する。

その解読され再生されたデータは、ＳＴＢ１００３に出力され、映像データであればＳＴＢ１００３に接続されているディスプレイに表示され、音声

データであればＳＴＢ１００３に接続されているディスプレイから出力される。

このように、例えばＡＶＨＤＤ１００１の蓄積手段１００６内の第１の記録媒体の記録可能容量が限界に達しようとしている場合であっても、蓄積手段１００６内のデータを上書きするなどして削除せずに、他の記録媒体にデータを移動させることができるので、後に移動させたデータを再生することができるというメリットがある。

また、不正行為によって、アーカイブ機器１００２に対応する、第２の記録媒体１０１０と同様のメディアが大量に複製され、そして配布されたとしても、そのメディアに記録されているデータは、ＡＶＨＤＤ１００１の暗号化手段１００４によって、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されたデータであるので、そのデータを再生することができるのはＡＶＨＤＤ１００１のみであり、著作権保護の対象データであるコピー禁止データを、著作権を保護して他の装置、つまりアーカイブ機器１００２に移動させることができる。したがって、安全なデータの移動を実現できるということである。なお、生産された複数のＡＶＨＤＤ１００１の固有の暗号化鍵は、それぞれ異なる。

なお、上述した実施の形態では、コピー禁止データは、ＡＶＨＤＤ１００１の暗号化手段１００４によって、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されるとしたが、コピー禁止データは、暗号化手段１００４によって暗号化されるものと限定することはない。例えば、ＡＶＨＤＤ１００１の製造段階で、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されたコピー禁止データが蓄積手段１００６内の第１の記録媒体に記録されていてもよい。

また、上述した実施の形態では、コピー禁止データは、暗号化手段１００４によって暗号化された後に蓄積手段１００６内の第１の記録媒体の記録されているとしたが、暗号化手段１００４が蓄積手段１００６と移動手段１００７との間に設けられており、コピー禁止データが、移動手段１００７によって移動させられるさいに、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されるとしてもよい。要するに、移動手段１００７が移動させようとするコピー禁止データは、少なくともＡＶＨＤＤ１００１から出力するさいに、そのＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されておりさえすればよい。

また、本実施の形態では、コピー禁止データは、他の記録装置への移動は許されているがコピーが禁止されているデータであるとしたが、「発明の実施の形態」における「コピー禁止データ」には、２ｂｉｔで「０１」と表される「これ以上コピー禁止」というデータや、２ｂｉｔで「１１」と表される「絶対的にコピー禁止」というデータも含まれる。

また、図２１を用いて説明した上記実施の形態の送信手段１０１１が、図２３に示すような、第２の記録媒体１０１０に記録されているデータを通常のN倍速（Nは１を超える正数）でＡＶＨＤＤ１００１に送信する高速送信手段１０１５に置き換えられていてもよい。その場合、図２１のＡＶＨＤＤ１００１を、データ格納手段としてのバッファ１０１４がさらに設けられているＡＶＨＤＤ１０１２に置き換えて、高速送信手段１０１５からのデータをバッファ１０１４に一時的に格納し、その一時的に格納されたデータを、再生手段１００８に再生させることができる。

そうすると、アーカイブ機器１０１３からＡＶＨＤＤ１０１２にN倍速（高速）でデータ転送をするとともに、ＡＶＨＤＤ１０１２においてデータを

通常再生することができるというメリットがでてくる。なお、バッファ１０１４は、蓄積手段１００６内に設けられていてもよい。また、「通常のN倍速」とは、再生手段１００８がデータを再生するさいの、ユーザが視聴するさいに必要なデータ再生速度よりも速い速度を意味する。

なお、図２３を用いて説明した例では、アーカイブ機器１０１３に高速送信手段１０１５を設けて、アーカイブ機器１０１３からＡＶＨＤＤ１０１２にN倍速（高速）でデータ転送するとしたが、ＡＶＨＤＤの移動手段１００７を、N倍速（Nは１を超える正数）でデータをアーカイブ機器に高速移動させる高速移動手段に置き換えてもよい。その場合、アーカイブ機器にはデータを一時的に格納するバッファを設けておくことが好ましい。このように、ＡＶＨＤＤに高速移動手段を設けておくと、ＡＶＨＤＤからアーカイブ機器に短時間でデータ移動を行わせることができるというメリットがでてくる。また、後述する実施の形態２におけるＡＶＨＤＤにおいても、移動手段の替わりに高速移動手段を設けると、短時間でデータ移動を行わせることができるという効果が現れる。

また、上述した実施の形態では、アーカイブ機器１００２には、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読し再生する手段は設けられていなかったが、図２３に示すように、アーカイブ機器１００２を、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読し再生する解読再生手段１０１７を備えたアーカイブ機器１０１６に置き換えて、ＡＶＨＤＤ１００１にデータ送信することなく、アーカイブ機器１０１６において、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読させ再生するとしてもよい。

このように、アーカイブ機器１０１６においてＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読し再生することができると、データを再生するためにのみアーカイブ機器１００２とＡＶＨＤＤ１００１とを接続しなければならないという問題は解消される。

なお、アーカイブ機器１０１６の解読再生手段１０１７が、暗号化されているデータを解読し再生するには、ＡＶＨＤＤ１００１固有の暗号化鍵が必要となるが、アーカイブ機器１０１６にＩＣカードスロットをあらかじめ設けておき、図２３に示すように、ＡＶＨＤＤ１００１固有の暗号化鍵が記録されているＩＣカード１０１８がＩＣカードスロットに挿入された場合に、解読再生手段１０１７がＩＣカード１０１８からＡＶＨＤＤ１００１固有の暗号化鍵を取得し、その暗号化鍵を用いて暗号化されているデータを解読し再生するとしてもよい。

また、ＩＣカード１０１８を用いる場合、解読再生手段１０１７とは別に、ＩＣカード１０１８を再生する鍵再生手段をアーカイブ機器１０１６に設けてもよい。また、ＩＣカード１０１８からのＡＶＨＤＤ１００１固有の暗号化鍵を記憶する鍵記憶手段をアーカイブ機器１０１６に設けてもよい。このように、アーカイブ機器１０１６に鍵記憶手段が設けられていると、第２の記録媒体１０１０に記録されている、ＡＶＨＤＤ１００１固有の暗号化鍵で暗号化されているデータを解読し再生するさい、その都度ＩＣカード１０１８がＩＣカードスロットに挿入されなければならないという問題を回避することができる。なお、ＩＣカード１０１８に記録されている鍵としては、鍵の漏洩を防止するために、秘密鍵と公開鍵とを組み合わせたものとすることができる。

また、上記の記載では、解読再生手段１０１７は、直接的にまたは間接的にＩＣカード１０１８からＡＶＨＤＤ１００１固有の暗号化鍵を取得するとしたが、解読再生手段１０１７は、ＩＣカード１０１８の替わりに、ＡＶＨＤＤ１００１固有の暗号化鍵が記録されているまたは埋め込まれているＫＥＹディスクやＫＥＹカセットから暗号化鍵を取得するとしてもよい。なお、第２の記録媒体１０１０に、ＡＶＨＤＤ１００１固有の暗号化鍵が記録されていてもよい。その場合、ＩＣカード１０１８や、ＫＥＹディスクや、ＫＥＹカセットは必要なくなる。

また、ＩＣカード１０１８、ＫＥＹディスクまたはＫＥＹカセットを用いるのではなく、ＡＶＨＤＤ１００１に、ＡＶＨＤＤ１００１固有の暗号化鍵を送信する手段を設けておくとともに、アーカイブ機器１０１６に、ＡＶＨＤＤ１００１からの暗号化鍵を受信する手段を設けておいて、解読再生手段１０１７が、送信されてきた暗号化鍵を用いて、暗号化されているデータを解読し再生するとしてもよい。

また、上述した実施の形態では、図２１に示したように、ＡＶＨＤＤ１００１は、アーカイブ機器１００２に暗号化されたデータを無条件で移動するとしたが、図２４に示すように、図２１のアーカイブ機器２の第２の記録媒体１０１０を、ＡＶＨＤＤ１０１９に対応する記録媒体であることを示す認証情報が記録されている第２の記録媒体１０２１に置き換え、それと同時にＡＶＨＤＤ１００１を、第２の記録媒体１０２１がＡＶＨＤＤ１０１９に対応する記録媒体であるか否かを判断する判断手段１０２０を備えたＡＶＨＤＤ１０１９に置き換えて、判断手段１０２０によって、第２の記録媒体１０２１がＡＶＨＤＤ１０１９に対応する記録媒体であると判断された場合に限

り、移動手段１００７が、ＡＶＨＤＤ１０１９からアーカイブ機器１００２にデータを移動させるとしてもよい。

なお、判断手段１０２０は、第２の記録媒体１０２１に認証情報が記録されていれば、第２の記録媒体１０２１がＡＶＨＤＤ１０１９に対応する記録媒体であるものと判断し、認証情報が記録されていなければ、第２の記録媒体１０２１がＡＶＨＤＤ１０１９に対応しないものと判断する。

ところで、認証情報が記録されている第２の記録媒体１０２１は、認証情報が記録されていない記録媒体と区別するために、認証情報が記録されていない記録媒体の表面の色とは異なる色を表面に有するディスクであるとしてもよく、また、著作権保護用の記録媒体であるので、認証情報が記録されていない記録媒体よりも所定の額だけ高価にしてもよい。そして、認証情報が記録されていない記録媒体の価格との差額の全部または一部が、著作権者または著作権団体に還元されるとしてもよい。

なお、第２の記録媒体１０２１がＡＶＨＤＤ１０１９に対応する記録媒体である場合にＡＶＨＤＤ１０１９からアーカイブ機器１００２にデータが移動されるのではなく、アーカイブ機器１００２がＡＶＨＤＤ１０１９に対応する装置である場合にＡＶＨＤＤ１０１９からアーカイブ機器１００２にデータが移動されるとしてもよい。その場合、ＡＶＨＤＤ１０１９には、アーカイブ機器１００２がＡＶＨＤＤ１０１９に対応する装置であるか否かを判断する判断手段が設けられることになる。

また、ＡＶＨＤＤ１００１とアーカイブ機器２とが接続されたインタフェースに、少なくともコピー禁止データの移動に対して課金能力を有する管理装置が接続されていることが確認されたときに、ＡＶＨＤＤ１００１の移動

手段１００７は、そのコピー禁止データをアーカイブ機器２に移動させるとしてもよい。なお、管理装置の一例としてはＳＴＢが挙げられる。

また、上述した実施の形態では、ＡＶＨＤＤからアーカイブ機器にコピー禁止データを移動させるとした。つまり、コピー禁止データをアーカイブ機器に移動させた後にはＡＶＨＤＤからコピー禁止データを削除するとした。しかしながら、アーカイブ機器においてコピー禁止データが処理できなくなることも考えられるので、コピー禁止データをＡＶＨＤＤにバックアップとして残しておくことが好ましい場合がある。

その場合、上述した実施の形態の各ＡＶＨＤＤの移動手段１００７を、コピー禁止データをアーカイブ機器にコピーする複写手段に置き換えると、アーカイブ機器にコピー禁止データを送信するとともに、ＡＶＨＤＤ内にコピー禁止データをバックアップ蓄積しておくことができ、アーカイブ機器においてコピー禁止データが処理できなくなった場合でも、ＡＶＨＤＤにバックアップ蓄積されたコピー禁止データを利用することができるというメリットが生まれる。

ここで、複写手段を備えたＡＶＨＤＤの構成の一例として、図２１に示す移動手段１００７を備えたＡＶＨＤＤ１００１を、移動手段１００７の替わりに複写手段１０８０を備えたＡＶＨＤＤ１０８１に置き換えた場合を例にとって、図２８に示す。

（第９の実施の形態）

次に、本発明の第９の実施の形態のＡＶＨＤＤ１０２２およびアーカイブ機器１０２３の構成を述べる。

図２５に、本発明の第９の実施の形態のＡＶＨＤＤ１０２２およびアーカ

イブ機器１０２３のブロック図を示す。なお、上記第８の実施の形態の図２１と同様に、説明の便宜上、図２５にはＳＴＢ１００３も表示している。

さて、本発明の第９の実施の形態のＡＶＨＤＤ１０２２は、図２５に示すように、ＳＴＢ１００３からのデータを蓄積手段１０２５内の記録媒体に記録する第３記録手段１０２４と、データを蓄積する蓄積手段１０２５と、蓄積手段１０２５に蓄積されているデータを平文化する平文化手段１０２６と、平文化手段１０２６によって平文化された、蓄積手段１０２５に蓄積されていたデータをアーカイブ機器１０２３に移動させる移動手段１０２７とで構成されている。

本発明の第９の実施の形態のアーカイブ機器１０２３は、図２５に示すように、ＡＶＨＤＤ１０２２からのデータをアーカイブ機器１０２３固有の暗号化鍵を用いて暗号化する暗号化手段１０２８と、暗号化手段１０２８によって暗号化されたデータを第３の記録媒体１０３０に記録する第４記録手段１０２９と、第３の記録媒体１０３０と、第３の記録媒体１０３０に記録されたデータをアーカイブ機器１０２３固有の暗号化鍵を用いて解読し再生する再生手段１０３１とで構成されている。なお、アーカイブ機器１０２３としては、例えばＤＶＤ装置や、Ｄ－ＶＨＳ装置が該当する。本実施の形態では、アーカイブ機器１０２３の一例としてＤＶＤ装置を用い、第３の記録媒体１０３０の一例としてはＤＶＤを用いる。

また、第９の実施の形態では、本発明の、データ処理装置の一例としてＡＶＨＤＤ１０２２を、記録再生装置の一例としてアーカイブ機器１０２３を、それぞれ用いる。

また、ＡＶＨＤＤ１０２２の蓄積手段１０２５内の記録媒体は、リムーバ

ブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。同様に、アーカイブ機器１０２３内の第３の記録媒体１０３０も、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。

また、ＡＶＨＤＤ１０２２とアーカイブ機器１０２３の接続は、図２１を用いて説明した第８の実施の形態と同様に、いずれのインターフェースを介して行われていてもよい。

次に、本発明の第９の実施の形態のＡＶＨＤＤ２２およびアーカイブ機器２３の動作を述べる。

ユーザによって、蓄積手段１０２５内のデータをアーカイブ機器１０２３内の第３の記録媒体１０３０に移動させるための指示が、ＡＶＨＤＤ１０２２およびアーカイブ機器１０２３に対してされたとする。なお、データの移動とは、第８の実施の形態で述べた通り、例えば第１の記録媒体に記録されているデータを、別の第２の記録媒体に移し、移した後には第１の記録媒体内には移ったデータを残さないことを意味する。

また、以下の説明の便宜上、移動対象のデータは、著作権保護のために、他の記録装置への移動は許されているがコピーが禁止されているコピー禁止データであって、第３記録手段１０２４によって蓄積手段１０２５内の記録媒体に記録されていたものであるとする。

さてこのとき、平文化手段１０２６は、蓄積手段１０２５に蓄積されているデータを平文化し、移動手段１０２７は平文のコピー禁止データを、蓄積手段１０２５内の記録媒体から読み出してアーカイブ機器１０２３に送信する。このようにして移動手段１０２７がコピー禁止データを送信するさい（移動させるさい）、その移動手段１０２７は、コピー禁止データを１回だけ

コピー可能なデータとして出力する。

そして、アーカイブ機器１０２３では、暗号化手段１０２８が、ＡＶＨＤＤ１０２２からのデータをアーカイブ機器１０２３固有の暗号化鍵を用いて暗号化し、第４記録手段１０２９が、暗号化手段１０２８によって暗号化されたデータを第３の記録媒体１０３０に記録する。なお、データは、アーカイブ機器１０２３に入力されたさい、もしくは第３の記録媒体１０３０に記録されたさいに、コピー禁止データとして扱われるものとする。

なお、ＡＶＨＤＤ１０２２からアーカイブ機器１０２３へのデータの伝送経路上では、例えばＤＴＣＰで伝送データは保護されるとしてもよい。

次に、第３の記録媒体１０３０に記録された、アーカイブ機器１０２３固有の暗号化鍵で暗号化されているコピー禁止データを再生する場合について説明する。その場合、再生手段１０３１は、アーカイブ機器１０２３固有の暗号化鍵を用いて、第３の記録媒体１０３０に記録されたコピー禁止データを再生することになる。

このように、アーカイブ機器１０２３では、アーカイブ機器１０２３固有の暗号化鍵でデータを暗号化し記録するので、アーカイブ機器１０２３内で、記録したデータを再生することができるというメリットがある。

なお、上述した実施の形態では、アーカイブ機器１０２３の暗号化手段１０２８は、ＡＶＨＤＤ１０２２からのコピー禁止データをアーカイブ機器１０２３固有の暗号化鍵を用いて暗号化するとしたが、第３の記録媒体１０３０に暗号化鍵が記録されている場合、暗号化手段１０２８は、第３の記録媒体１０３０に記録されている暗号化鍵を用いて、ＡＶＨＤＤ１０２２からのコピー禁止データを暗号化するとしてもよい。この場合、再生手段１０３１

は、第３の記録媒体１０３０に記録されている暗号化鍵用いて、コピー禁止データを再生することになる。

また、上述した実施の形態では、ＡＶＨＤＤ１０２２からアーカイブ機器１０２３へ移動するデータは平文データであるとしたが、移動データは、アーカイブ機器１０２３固有の暗号化鍵で暗号化されたデータであってもよいし、第３の記録媒体１０３０に暗号化鍵が記録されている場合、その第３の記録媒体１０３０に記録されている暗号化鍵で暗号化されたデータであってもよい。

その場合、ＡＶＨＤＤ１０２２には、アーカイブ機器１０２３固有の暗号化鍵を用いて、または第３の記録媒体１０３０に記録されている暗号化鍵を用いて、コピー禁止データを暗号化する暗号化手段が設けられることになる。また、ＡＶＨＤＤ１０２２には、アーカイブ機器１０２３固有の暗号化鍵をアーカイブ機器１０２３から取得する手段や、第３の記録媒体１０３０に記録されている暗号化鍵をアーカイブ機器１０２３から取得する手段が設けられることになる。なお、アーカイブ機器１０２３からは、暗号化手段２８が不要となる。

また、ＡＶＨＤＤ１０２２からアーカイブ機器１０２３へ移動するデータは、アーカイブ機器１０２３において用いられるフォーマットのデータであってもよい。その場合、ＡＶＨＤＤ１０２２には、移動させるデータをアーカイブ機器１０２３用のフォーマットのデータに変換するフォーマット変換手段が設けられるとすることができる。また、ＡＶＨＤＤ１０２２において蓄積手段１０２５内にデータを記録するさい、そのデータは、アーカイブ機器１０２３において用いられるフォーマットで記録されるとしてもよい。

また、第８の実施の形態において図２４を用いて説明したように、ＡＶＨＤＤ１０２２に、第３の記録媒体１０３０がＡＶＨＤＤ１０２２に対応する記録媒体であるか否かを判断する判断手段を設けて、その判断手段によって、第３の記録媒体１０３０がＡＶＨＤＤ１０２２に対応する記録媒体であると判断された場合に、移動手段１０２７は、平文のまたは暗号化されたコピー禁止データをアーカイブ機器１０２３に移動させるとしてもよい。

なお、第３の記録媒体１０３０に、その第３の記録媒体１０３０がＡＶＨＤＤ１０２２に対応する記録媒体であることを示す鍵が付されている場合、ＡＶＨＤＤ１０２２に設けられる判断手段は、第３の記録媒体１０３０に付されている鍵を利用して、第３の記録媒体１０３０がＡＶＨＤＤ１０２２に対応する記録媒体であるか否かを判断するとしてもよい。

また、第３の記録媒体１０３０がＡＶＨＤＤ１０２２に対応する記録媒体であるか否かを判断してデータ移動を行うのではなく、アーカイブ機器１０２３がＡＶＨＤＤ１０２２に対応する装置であるか否かを判断してデータ移動を行ってもよい。その場合、ＡＶＨＤＤ１０２２には、アーカイブ機器１０２３がＡＶＨＤＤ１０２２に対応する装置であるか否かを判断する判断手段が設けられることになり、その判断手段によって、アーカイブ機器１０２３がＡＶＨＤＤ１０２２に対応する装置であると判断された場合に、移動手段１０２７は、平文のまたは暗号化されたコピー禁止データをアーカイブ機器１０２３に移動させるとしてもよい。

なお、アーカイブ機器１０２３がＡＶＨＤＤ１０２２に対応する装置であるかことを示す鍵を有している場合、ＡＶＨＤＤ１０２２に設けられる判断手段は、アーカイブ機器１０２３が有している鍵を利用して、アーカイブ機

器１０２３がＡＶＨＤＤ１０２２に対応する装置であるか否かを判断するとしてもよい。

また、ＡＶＨＤＤ１０２２とアーカイブ機器１０２３とが接続されたインタフェースに、少なくともコピー禁止データの移動に対して課金能力を有する管理装置が接続されていることが確認されたときに、ＡＶＨＤＤ１０２２の移動手段１０２７は、そのコピー禁止データをアーカイブ機器１０２３に移動させるとしてもよい。なお、管理装置の一例としてはＳＴＢが挙げられる。

また、第８の実施の形態および２の各ＡＶＨＤＤには、データの移動を行ったさい、そのデータの移動に対する課金情報を、各ＡＶＨＤＤを管理する管理装置に送信する手段が設けられていてもよい。また、管理装置の一例として、課金を行う手段が組み込まれているＳＴＢ１００３を用いることができる。

また、上述した実施の形態では、ＡＶＨＤＤからアーカイブ機器にコピー禁止データを移動させるとした。つまり、コピー禁止データをアーカイブ機器に移動させた後にはＡＶＨＤＤからコピー禁止データを削除するとした。しかしながら、アーカイブ機器においてコピー禁止データが処理できなくなることも考えられるので、コピー禁止データをＡＶＨＤＤにバックアップとして残しておくことが好ましい場合がある。

その場合、上述した実施の形態のＡＶＨＤＤの移動手段１０２７を、コピー禁止データをアーカイブ機器にコピーする複写手段に置き換えると、アーカイブ機器にコピー禁止データを送信するとともに、ＡＶＨＤＤ内にコピー禁止データをバックアップ蓄積しておくことができ、アーカイブ機器におい

てコピー禁止データが処理できなくなった場合でも、ＡＶＨＤＤにバックアップ蓄積されたコピー禁止データを利用することができるというメリットが生まれる。

ここで、複写手段を備えたＡＶＨＤＤの構成の一例として、図２４に示す移動手段１００７を備えたＡＶＨＤＤ１０２２を、移動手段１０２７の替わりに複写手段１０９０を備えたＡＶＨＤＤ１０９１に置き換えた場合を例にとって、図２９に示す。

（第１０の実施の形態）

次に、本発明の第１０の実施の形態の暗号化データ復号記録システムについて説明する。

図３０に、本第１０の実施の形態の暗号化データ復号記録システムの構成を示す。図３０に示すように、本第１０の実施の形態の暗号化データ復号記録システムは、５個の記録装置１１００ａ～１１００ｅと、復号記録装置１１０１とで構成されている。

図３１に本第１０の実施の形態における各記録装置１１００の構成を示す。図３１に示すように、各記録装置１１００は、記録手段１１０２と、その記録手段１１０２に記録されているデータを出力する出力手段１１０３とを有している。ここで、記録手段１１０２に記録されているデータは、コピーが禁止されているコピー禁止データが暗号化されたデータであって、各記録装置１１００の記録手段１１０２には、同じ内容の暗号化されたコピー禁止データが記録されているものとする。

次に、図３２に本第１０の実施の形態における復号記録装置１１０１の構成を示す。図３２に示すように、復号記録装置１１０１は、復号手段１１０

４と、記録手段１１０５とを有している。ここで、復号手段１１０４は、記録装置１１００から出力される暗号化されたコピー禁止データを復号する手段であって、記録手段１１０５は、記録装置１１００に記録されているコピー禁止データと同じ内容のデータであって、暗号化されているコピー禁止データ、または暗号化されていないコピー禁止データを記録する手段である。

ところで、上述した本第１０の実施の形態の暗号化データ復号記録システムでは、同じ内容のデータが、５個の記録装置１１００ａ～１１００ｅ、および復号記録装置１１０１それぞれに記録されているが、暗号化されたコピー禁止データは、復号記録装置１１０１の復号手段１１０４でしか復号され得ない。

したがって、本第１０の実施の形態の暗号化データ復号記録システムを用いると、著作権を保護しつつ、データをその著作権を保護すべきデータをバックアップしておくことができるという効果が現れる。

なお、上述した実施の形態における暗号化データ復号記録システムは、記録装置１１００は、ａ～１１００ｅを備えているとしたが、記録装置１１００の個数は５個に限定されるものではない。要するに複数個存在しておりさえすればよい。

（第１１の実施の形態）

次に、本発明の第１１の実施の形態のＡＶＨＤＤ１０３２について説明する。なお第１１の実施の形態では、ＡＶＨＤＤ１０３２からのデータの送信について述べるが、その送信するデータはＤＶＤ装置１０３３のＤＶＤ１０３７に記録されるものとする。

図２６に、本発明の第１１の実施の形態のＡＶＨＤＤ１０３２およびＤＶ

D装置１０３３のブロック図を示す。

さて、本発明の第１１の実施の形態のＡＶＨＤＤ１０３２は、図２６に示すように、データを蓄積する蓄積手段１０３４と、蓄積手段１０３４に蓄積されているデータをＤＶＤ装置１０３３に送信する送信手段１０３５とで構成されている。

本発明の第１１の実施の形態のＤＶＤ装置１０３３は、図２６に示すように、ＡＶＨＤＤ１０３２からのデータをＤＶＤ１０３７に記録する第５記録手段１０３６と、第５記録手段１０３６に記録されたデータを再生する再生手段１０３８とで構成されている。

なお、第１１の実施の形態では、本発明の、データ送信装置の一例としてＡＶＨＤＤ１０３２を用いる。

また、ＡＶＨＤＤ１０３２とＤＶＤ装置１０３３の接続は、どのようなインターフェースを介して行われていてもよい。

次に、本発明の第１１の実施の形態のＡＶＨＤＤ１０３２およびＤＶＤ装置１０３３の動作を述べる。

ここで、ＡＶＨＤＤ１０３２が送信するデータは、複数個のデータパケットで構成されているストリームであるとする。図２７に、そのストリームの一部の構成を示す。ストリームは、図２７に示すような、Ｄ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４の５個のデータパケットで構成されるブロック複数個で構成されるストリームであって、Ｄ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４それぞれは、数字が大きくなる順番で時間的に連続するデータパケットであって、時間上の一つ手前のデータが再生されないと再生されないようになっている、連鎖暗号化されたデータである。

したがって、データパケットＤ０、Ｄ１、Ｄ２を取り上げると、データパケットＤ０の時間的に後に続くものがデータパケットＤ１であって、その次に続くものがデータパケットＤ２ということになり、データパケットＤ１は、データパケットＤ０が再生されないと再生されず、データパケットＤ２は、データパケットＤ１が再生されないと再生されないようになっている。

このようなストリームを、ＡＶＨＤＤ１０３２がＤＶＤ装置１０３３に送信するさいの動作についてであるが、ＡＶＨＤＤ１０３２の送信手段１０３５は、蓄積手段１０３４に蓄積されているストリームをＤＶＤ装置１０３３に送信するさい、ストリームを構成する各ブロックのデータパケットを、Ｄ４、Ｄ３、Ｄ２、Ｄ１、Ｄ０の順序で送信する。

ＤＶＤ装置１０３３では、第５記録手段１０３６が、ＡＶＨＤＤ１０３２からのデータをＤＶＤ１０３７に記録する。

ＤＶＤ１０３７に記録されたデータを再生するときは、再生手段１０３８が、ストリームを構成する各ブロックについて、データパケットを、Ｄ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４の順に再生していき、ストリーム全体を再生する。

このように、ＡＶＨＤＤ１０３２からＤＶＤ装置１０３３に送信されるデータパケットが、Ｄ４、Ｄ３、Ｄ２、Ｄ１、Ｄ０の順に送信されるので、データ送信の途中に停電などで電源遮断されても、Ｄ４、Ｄ３、Ｄ２、Ｄ１、Ｄ０が送信されなければ、データパケットＤ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４で構成されるブロックは再生されないので、送信データが他の装置に漏れた場合であっても、その送信データが他の装置において解読されるという状況を回避することができる。

なお、上述した実施の形態では、データパケットＤ０、Ｄ１、Ｄ２、Ｄ３

、Ｄ４の連鎖暗号化について詳述しなかったが、連鎖暗号化されたデータパケットＤ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４がＡＶＨＤＤ１０３２の蓄積手段１０３４に蓄積されていてもよいし、ＡＶＨＤＤ１０３２に連鎖暗号化を行う手段を設けて、ＡＶＨＤＤ１０３２の送信手段１０３５がストリームを送信しようとするさいに、各ブロックのデータパケットそれぞれについて連鎖暗号化させるようにしてもよい。

また、上述した実施の形態では、ストリームは、Ｄ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４の５個のデータパケットで構成されるブロック複数個で構成されるとしたが、各ブロックを構成するデータパケットの数は５個に限定されるものではない。また、ストリームは、複数個のブロックで構成されると限定されるものでもない。ストリームは、複数個のブロックで構成されておらず、複数個のデータパケットで構成されていてもよい。その場合、送信手段１０３５は、ストリームを構成するデータパケットを、最後尾から先頭側に順に送信することになる。

また、上述した実施の形態では、ストリームの送信について説明したが、ストリームを移動させる場合には、データパケットＤ０、Ｄ１、Ｄ２、Ｄ３、Ｄ４について着目すると、データパケットＤ４、Ｄ３、Ｄ２、Ｄ１の転送が完了したら、移動前の記録媒体からデータパケットＤ１～Ｄ４を消去し、その消去が完了した後にデータパケットＤ０を転送し、移動前の記録媒体からデータパケットＤ０を消去するとしてもよい。

なお、以上第８～第１１の実施の形態では、ＣＣＩの値が、Ｃｏｐｙ　Ｎｅｖｅｒ、Ｃｏｐｙ　ｏｎｃｅ、Ｎｏ　ｍｏｒｅ　ＣｏｐｙのいずれかであるＡＶデータを一括してコピー禁止データと呼んだが、以下第１２～第１６

の実施の形態では、ＣＣＩがＣｏｐｙ　ｎｅｖｅｒであるＡＶデータなどの複製することが禁止されているコンテンツを複製禁止コンテンツと呼ぶことにする。

（第１２の実施の形態）

図３３は、本発明の第１２の実施の形態による記録再生装置の構成図である。図に示すように、判別情報検出手段２０１０は、外部からの放送信号から、コピー制限に関する判別情報を検出するための手段、時間情報取得手段２０１１は、外部の放送信号から、時間に関する時間信号を取得するための手段、記録再生手段２０１２は、外部からの放送信号を記録再生するための手段、記録媒体２０１３は、ハードディスク等で実現される、記録再生が同時に可能であり、ランダム・アクセスが可能である、放送のデータを蓄積するための手段、制御入力インターフェイス（以下制御入力Ｉ／Ｆ）２０１５は、ユーザからの制御を受け付ける手段、切り替え手段２０１６は、記録再生手段２０１２からの入力と、外部からの放送の入力とを受け、いずれかを選択して外部のモニタ等へ出力する手段である。また、記録媒体２０１３において、記録バッファ２０１４は、コピー制限がなされたデータを専用に記録する領域である。なお、本実施の形態にて扱われる放送は、ＭＰＥＧトランスポートストリームまたはＭＰＥＧプログラムストリーム（以下総称してＭＰＥＧストリームと呼ぶ）を用いたデジタル放送であり、デコード処理に関する手段等は省略するものとする。以下、各実施の形態も同様である。また、判別情報検出手段２０１０，時間情報取得手段２０１１，記録再生手段２０１２は本発明の記録手段の一例である。

以上のような構成を有する、本発明の第１２の実施の形態による記録再生

装置の動作について、以下に説明を行う。

はじめに、判別情報検出手段２０１０は、外部からＭＰＥＧストリームの入力を受けると、ヘッダまたはデータ列を構成する各パケットを参照して、コピーガードもしくはＣＣＩ（Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）等の著作権に関する情報を検出し、入力したコンテンツが、コピー禁止またはコピー制限が施されているものかどうかを判断する。今回の場合は、コピー禁止とされた複製禁止コンテンツのみが入力されているものとする。

次に、入力したＭＰＥＧストリームが、複製禁止コンテンツであることが判明すると、判別情報検出手段２０１０は、記録再生手段２０１２に対し、検出情報を出力する。検出情報の例としては、ＭＰＥＧストリームに含まれる著作権情報や、コピーガード等がある。記録再生手段２０１２は、検出情報を受けると、これに基づき、記録媒体２０１３内の記録バッファ２０１４にＭＰＥＧストリームを記録するための準備を行う。

外部から、判別情報検出手段２０１０を介してＭＰＥＧストリームが入力すると、記録再生手段２０１２は、これを記録バッファ２０１４に記録する。

次に、記録再生手段２０１２による記録バッファ２０１４への記録動作の詳細について説明を行う。図３４は、本第１２の実施の形態による記録再生装置の動作を説明するためのタイムチャートである。図に示すように、本実施の形態の動作例として、記録バッファ２０１４に対し、放送時間９０分に相当するデータ量を一時的に記録するための本実施の形態の記録再生装置を用い、生放送期間２０２０に放送されている放送時間１２０分の複製禁止コンテンツに対し、放送開始時刻から９０分経過した後にタイムシフト再生に

よる視聴を行うものとする。

はじめに、放送開始時刻になると、記録再生手段２０１２は記録バッファ２０１４に複製禁止コンテンツを構成するデータの記録を開始する。放送開始時刻以降、記録再生手段２０１２は、記録バッファ２０１４にデータを逐次記録し続けるが、再生は行わない。

一方、時間情報取得手段は、ＭＰＥＧストリームから、ＰＣＲパケットやタイムスタンプなどの時間情報を取得して、記録再生手段２０１２が複製禁止コンテンツを記録バッファ２０１４に記録開始した時点から、記録時間の計測を開始する。

次に、放送開始時刻から、時間情報取得手段２０１１の計測により記録期間２０２１（９０分）が経過すると、記録再生手段２０１２は、外部から入力されるＭＰＥＧストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ２０１４上から消去開始する。ただし、今回の動作例においては、放送開始時刻から記録期間２０２１が経過した時刻は、タイムシフト再生による視聴期間２０２４が始まる視聴開始時刻となっているため、記録再生手段２０１２は、記録されたデータを消去する前に再生し、切り替え手段２０１６を介して外部モニタへ出力する。

すなわち、記録期間２０２１において記録されたデータのうち、最初の３０分の部分２０２２ａに相当するデータ（生放送期間２０２０ａに放送されたコンテンツ）は、放送開始時刻から９０分経過後、タイムシフト再生による視聴開始時刻とともに、再生（タイムシフト再生による視聴期間２０２４ａにて視聴されるコンテンツ）が行われ、その後直ちに消去されることになる。

次に、タイムシフト再生による視聴開始時刻から記録再生期間２０２２ａが経過すると、記録再生手段２０１２は、記録再生期間２０２２ｂとして、データの逐次記録を放送終了時刻まで継続するとともに、既に記録バッファ２０１４内に蓄積したデータの再生を、データ部分２０２２ａから連続するようにして継続する。

次に、放送終了時刻になると、記録再生手段２０１２は、データの逐次記録を停止し、記録バッファ２０１４に記録されているデータの再生を、視聴終了時刻まで実行する（再生期間２０２３）。

なお、以上の動作について、記録再生期間２０２２ｂおよび再生期間２０２３においては、再生したデータは一旦記録バッファ２０１４上に保存しておいて、視聴終了時刻経過後、一括して消去するようにしてもよいが、事故により記録再生装置の電源が切れた場合など、データが記録媒体２０１３上に保存されてしまう事態を防ぐために、再生した直後に消去するのが望ましい。

また、視聴開始時刻を経過しても、タイムシフト再生が行われない場合は、記録再生手段２０１２は記録バッファ２０１４上に記録した全てのデータを消去する。これにより、複製禁止コンテンツをタイムシフト以外の形式で再生されることを防ぐことができる。

また、以上の説明においては、判別情報検出手段２０１０が複製禁止コンテンツのデータに含まれる判別情報を検出すると、記録再生手段２０１２が自動的にタイムシフト再生のための記録動作を開始するものとして説明を行ったが、記録再生手段２０１２の記録動作開始は、判別情報をきっかけとするものでなく、制御入力Ｉ／Ｆ２０１５を介して、外部（ユーザ）からの制

御によって行われるものとしてもよい。

また、以上の説明においては、記録期間２０２１の終了とタイムシフト再生による視聴開始時刻とを同時刻に設定し、複製禁止コンテンツのタイムシフト再生の動作と、該複製禁止コンテンツを構成するデータの消去の動作とを連動するものとして説明を行ったが、これに限定する必要はなく、図３５に示すように、視聴開始時刻は、記録期間２０２１内（タイムシフト再生を任意の時刻に設定可能な期間２０２４ｃ）でさえあれば、制御入力Ｉ／Ｆ２０１５からの制御に基づき、任意の時刻に設定してよいし、時刻設定を行わず、記録再生手段２０１２への直接命令によって実行してもよい。このとき、記録期間２０２１内に、記録再生手段２０１２へのタイムシフト再生の直接命令が行われない場合は、記録再生手段２０１２は記録動作を停止するようにするのが好ましい（図３５中の期間２０２１ａ）。また同時に、再びタイムシフト再生の直接命令が行われても、これを受付けないように設定するのが望ましい。

また、以上の動作において、記録期間２０２１を経過した場合、記録再生手段２０１２は、外部から入力されるＭＰＥＧストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ２０１４上から消去するものとして説明を行ったが、再生不可能な状態に該データを書き換えた上で、記録バッファ２０１４上にデータを保持しておくようにしてもよい。

（第１３の実施の形態）

本発明の第１３の実施の形態による記録再生装置は、複製禁止コンテンツを記録するための記録バッファとして、リングバッファを用いたものである。

図３６は、本発明の本第１３の実施の形態による記録再生装置の構成図である。図において、図３３と同一部または相当部については、同一符号を附し説明を省略する。また、リングバッファ２０４４は、同一領域に上書き記録を繰り返し行うことにより一定量のデータを一時記録する手段である。

以上のような構成を有する、本発明の第１３の実施の形態による記録再生装置について、以下、その動作を説明する。

はじめに、判別情報検出手段２０１０が、外部のＭＰＥＧプログラムストリームを参照して、複製禁止コンテンツを記録再生手段２０１２がリングバッファ２０４４に記録する動作については、第１２の実施の形態と同様に行われる。

次に、記録再生手段２０１２による、リングバッファ２０４４への記録動作の詳細について説明を行う。先に説明したように、リングバッファ２０４４は、記録媒体２０１３上の特定領域であって、一定量のデータを記録すると、記録開始位置に戻って上書き記録を行うものである。このとき、リングバッファ２０４４の大きさは、あらかじめ設定しておいてもよいし、判別情報検出手段２０１０から取得した検出情報に基づいて設定されるようにしてもよいが、いずれの場合でも、リングバッファ２０４４の大きさは、記録の対象となる複製禁止コンテンツを全て記録できないように設定される。例えば、複製禁止コンテンツの放送時間が１２０分であるとすれば、リングバッファ２０４４は９０分に相当する容量に設定されるようにする。

上記のように設定されたリングバッファ２０４４に対し、記録再生手段２０１２が複製禁止コンテンツの記録を開始する。

ここで図３７は、本第１３の実施の形態による記録再生装置の動作を説明

するためのタイムチャートである。以下、図３７を参照して、本第１３の実施の形態の記録再生手段２０１２とリングバッファ２０４４との動作の詳細を説明する。ただし、図に示すように、本実施の形態の動作例の各時刻、各時間の設定は、図３４に示す第１２の実施の形態の場合と同様とする。

はじめに、放送開始時刻になると、記録再生手段２０１２はリングバッファ２０４４に複製禁止コンテンツを構成するデータの記録を開始する。放送開始時刻以降、記録再生手段２０１２はリングバッファ２０４４に設定した容量がいっぱいになるまでデータを逐次記録し続けるが、再生は行わない（記録期間２０５１）。

次に、放送開始時刻から記録期間２０５１が経過し、リングバッファ２０４４に設定した容量がいっぱいになると、記録再生手段２０１２は、リングバッファ２０４４上において、記録期間２０５１の時点の記録位置から、記録開始位置に記録ヘッド（リングバッファポインタ）を戻し、新たなデータの上書き記録を行う。

また、今回の動作例においては、記録期間２０５１の終了は、タイムシフト再生による視聴期間２０５４の開始時刻と同一であるから、記録再生手段２０１２は、外部から入力されるＭＰＥＧストリームの上書き記録を行うとともに、放送開始時刻から記録された、上書き直前のデータの再生を開始する。すなわち、記録期間２０５１において記録されたデータのうち、最初の３０分の部分２０５２ａに相当するデータ（生放送期間２０５０ａに放送されたコンテンツ）は、放送開始時刻から９０分経過後、タイムシフト再生による視聴開始時刻とともに再生され、上書き記録により消去される。。

続いて、記録再生手段２０１２は、データの逐次記録を放送終了時刻まで

継続するとともに、データ再生を継続する（記録再生期間２０５２ｂ）。

次に、放送終了時刻になると、記録再生手段２０１２は、データの上書き記録を停止し、リングバッファ２０４４に記録されているデータの再生を、視聴終了時刻まで実行する（再生期間２０５３）。

なお、以上の動作について、リングバッファ２０４４から再生したデータは、一旦リングバッファ２０４４上に保存しておいて、視聴終了時刻経過後、一括して消去するようにしてもよいが、事故により記録再生装置の電源が切れた場合など、データが記録媒体２０１３上に保存されてしまう事態を防ぐために、再生した直後に消去するのが望ましい。

また、視聴開始時刻を経過しても、タイムシフト再生が行われない場合は、記録再生手段２０１２はリングバッファ２０４４上に記録した全てのデータを消去する。これにより、複製禁止コンテンツをタイムシフト以外の形式で再生されることを防ぐことができる。

また、以上の動作においては、記録期間２０５１の終了とタイムシフト再生による視聴開始時刻とを同時刻に設定し、複製禁止コンテンツのタイムシフト再生の動作と、該複製禁止コンテンツを構成するデータの上書き記録の動作とを連動するものとして説明を行ったが、これに限定する必要はなく、図３８に示すように、視聴開始時刻は、記録期間２０６１内（タイムシフト再生を任意の時刻に設定可能な期間２０６４ｃ）でさえあれば、制御入力Ｉ／Ｆ２０１５からの制御に基づき、任意の時刻に設定してよいし、時刻設定を行わず、記録再生手段２０１２への直接命令によって実行してもよい。このとき、記録期間２０６１内に、記録再生手段２０１２へのタイムシフト再生の直接命令が行われない場合は、記録再生手段２０１２は記録動作を停止

するようにするのが好ましい（図中の期間２０６１ａ）。また同時に、再びタイムシフト再生の直接命令が行われても、これを受付けないように設定することが望ましい。

また、以上の動作においては、記録期間２０６１を経過した場合、記録再生手段２０１２は、外部から入力されるＭＰＥＧストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ２０１４上から消去するものとして説明を行ったが、再生不可能な状態に該データを書き換えた上で、記録バッファ２０１４上にデータを保持しておくようにしてもよい。

また、本実施の形態によるタイムシフト再生において、データを再生する際のリングバッファ上の記録位置については、（１）リングバッファ２０４４上に上書き記録が行われていない状態での再生位置は、リングバッファ２０４４上にて記録が開始された位置と同一となり、（２）上書き記録が行われている状態での再生位置は、リングバッファ２０４４上にて、再生動作の制御が行われた時点の位置（上書き記録が最後に行われた位置）の直後となるようにする。すなわち、上記（１）（２）のいずれの場合においても、タイムシフト再生は、リングバッファ２０４４に記録されたもっとも古いデータから順に読み出しが行われるようにする。図３８に示す例では、上記（１）は、期間２０６４ｄ（放送開始時刻以降３０分）内にタイムシフト再生が行われた場合に相当し、再生開始位置は常に図中点Ａに一意に決定される。上記（２）は、期間２０６４ｅ（放送開始時刻３０分経過以降６０分まで）内にタイムシフト再生が行われた場合に相当し、再生開始位置は、期間２０６４ｅ上のリングバッファの記録ヘッド（バッファポインタ）の現在位置に

相当する。

（第１４の実施の形態）

本発明の第１４の実施の形態による記録再生装置は、複製禁止コンテンツと、複製可能なコンテンツとが混在する放送を受信する場合、複製禁止コンテンツだけを選択的にタイムシフト再生できるようにしたものである。

本実施の形態の構成は第１２の実施の形態と同様であるので、説明には図３３を用いる。また、図３９は、本実施の形態による記録再生装置の動作を説明するための図である。ただし、本実施の形態においては、タイムシフト可能な時間を上記実施の形態の９０分ではなく、１２０分に設定したものとする。以下、図３９を参照して、本発明の実施の形態の動作を説明する。

外部から入力されるＭＰＥＧストリーム２０７０は、コピーが禁止された複製禁止コンテンツ２０７０ａおよび２０７０ｃと、コピー可能な通常のコンテンツ２０７０ｂおよび２０７０ｄとが混在しており、時系列順に、複製禁止コンテンツ２０７０ａ、コンテンツ２０７０ｂ、複製禁止コンテンツ２０７０ｃ、コンテンツ２０７０ｄの順に記録再生装置に入力する。判別情報検出手段２０１０は、各コンテンツに含まれる判別情報を取得して、記録再生手段２０１２に出力し、時間情報取得手段は、各コンテンツ毎に時間情報を記録再生手段２０１２へ出力する。判別情報および時間情報を取得した記録再生手段２０１２は、これらに基づき、各コンテンツの放送時間が経過する毎に、複製禁止コンテンツは記録バッファ２０１４に一時記録し、通常のコンテンツは記録媒体２０１３内の、記録バッファ以外の記録領域に記録するようにする。

このとき、コンテンツの入力は時系列順となるので、図３９に示すように

、記録バッファ２０１４においては、はじめに複製禁止コンテンツ２０７０ａ、次いで複製禁止コンテンツ２０７０ｃが記録され、記録媒体２０１３においては、はじめにコンテンツ２０７０ｂ、次いでコンテンツ２０７０ｄが記録される。

記録バッファ２０１４内に記録された複製禁止コンテンツ２０７０ａおよび２０７０ｃは、第１２の実施の形態と同様にして順々にタイムシフト再生される。タイムシフト再生終了後には記録バッファ２０１４からはデータが消去、または再生不可能な状態にされるが、記録媒体２０１３内に記録されたコンテンツ２０７０ｂおよび２０７０ｄは、恒久的に記録しておくことができる。

なお、上記の説明においては、本実施の形態は、第１２の実施の形態の構成を有する記録再生装置において実現されるものとして説明を行ったが、第１３の実施の形態の構成とした場合でも、同様に行うことができる。

（第１５の実施の形態）

本発明の第１５の実施の形態による記録再生装置は、一時的に記録された複製禁止コンテンツのデータを暗号化して、視聴することが不可能な状態にするものである。

図４０は、本発明の第１５の実施の形態の記録再生装置に用いられるデータ秘匿化手段２０８０の構成図である。図に示すように、記録バッファ２０１４は第１２の実施の形態の記録バッファと同一手段、暗号化手段２０８１は記録再生手段２０１２から入力されるデータを時変キーにより暗号化する手段、復号化手段２０８２は記録バッファ２０１４から出力される暗号化されたデータを復号する手段、時変キー生成手段２０８３は暗号化手段２０８

１および復号化手段２０８２にて用いる時変キーを生成する手段、キーバッファ２０８４は時変キーを一時蓄積する手段である。

以上のような構成を有する本実施の形態の動作を、以下に説明する。記録再生手段２０１２からデータが暗号化手段２０８１に入力されると、暗号化手段２０８１は、時変キー生成手段２０８３が生成した時変キーに基づき元データを暗号化する。暗号化されたデータは記録バッファ２０１４に記録される。

一方、時変キー生成手段８３は、暗号化手段２０８１が取得したものと同じ時変キーをキーバッファ２０８４に出力し、キーバッファ２０８４はこれを保持しておく。

次に、記録再生手段２０１２がタイムシフト再生を行い、記録バッファから暗号化したデータを復号化手段２０８２に出力すると、復号化手段はキーバッファ２０８４からデータの復号に必要なデータを取得して、該データの復号を行う。

上記の動作において、時変キーを一時的に格納するキーバッファは、記録バッファ２０１４のデータ容量の時間分と同一の時間分が越えると消滅するようにする。これにより、タイムシフト再生が行われなかったデータは、暗号化されたまま記録バッファ２０１４内に保持されることになり、再生することは可能でも、視聴することは不可能になる。

時変キーを消滅させるには、例えば、キーバッファ２０８４を、リングバッファ構成としておいて、キーバッファに蓄積されていくキーを常に新しいもので上書きするようにするとよい。リングバッファの容量としては、例えば、図３４に示す第１２の実施の形態の動作例であるならば、記録期間２０

２１と同等とする。

また、タイマーを別途設けて時間を計測しておき、所定の時刻が経過するとキーバッファ２０８４から、設定した時刻以降のキーを逐次消去するようにしてもよい。

また、キーバッファ２０８４を揮発性メモリによって構成すると、記録再生装置の電源をオフにすると、キーバッファ内の全てのキーが消去され、これによっても秘匿性を確保することが可能となる。

（第１６の実施の形態）

本発明の第１６の実施の形態による記録再生装置は、タイムシフト再生のタイミングを、ユーザに告知できるようにしたものである。

図４１は、本発明の本第１６の実施の形態による記録再生装置の構成図である。図において、図３３と同一部または相当部については、同一符号を附し説明を省略する。また、告知手段２０９１は、音声、画像または文字情報によって、該記録再生装置の動作状態を告知するための手段である。

また、図４２は、本実施の形態による記録再生装置の動作を説明するための図である。以上のような構成を有する、本発明の第１６の実施の形態による記録再生装置について、以下、その動作を説明する。ただし、記録バッファ２０１４に設定する容量は、第１２の実施の形態と同様、放送時間９０分に相当するものとし、その他、第１２の実施の形態と重複する動作については説明を省略し、相違点のみを述べる。

はじめに、ユーザが放送局から放送される複製禁止コンテンツを生放送にて視聴しており、時刻ｔに何らかの理由で視聴を一時中断する場合を考える。このとき、ユーザは制御入力Ｉ／Ｆ２０１５から入力を行い、記録再生手段

２０１２を起動させる。記録再生手段２０１２は、制御入力Ｉ／Ｆ２０１５からの入力を受けた時点（時刻ｔ１と同一）から、記録バッファ２０１４に該複製禁止コンテンツの記録を開始する。一方、この間記録再生装置は「ポーズ」状態となる。

記録バッファ２０１４には、第１２の実施の形態の動作と同様にして、複製禁止コンテンツのデータが記録されていくが、時刻ｔ２になると、ユーザに対してアラーム音を発しユーザに対して記録再生装置に対して制御を行うよう注意を促す。本実施の形態においては、時刻ｔ２は、記録時刻ｔ１から、記録再生手段２０１２が記録バッファ２０１４に記録しているデータの、設定した容量に達するまでの残りの量（放送時間単位）と設定してあり、本実施の形態では（放送時間単位で）５分とした。したがって時刻ｔ２は、具体的には（記録開始（ポーズ開始）時刻＋８５分（記録バッファに一時記録された複製禁止コンテンツの量－５分））となる。

告知手段２０９１からの告知によって、ユーザは、制御入力Ｉ／Ｆ２０１５から入力を行い、ポーズを解除して、複製禁止コンテンツの視聴を再開する。ポーズ前と異なるのは、ユーザが視聴している複製禁止コンテンツは、放送局からの生放送ではなく、記録バッファ２０１４からタイムシフト再生されたものということである。

この場合、時刻ｔ２から時刻ｔ１までの間ポーズが行われることとなり、ユーザの番組視聴終了時刻ｔ６は、実際の放送の終了時刻ｔ４よりこの（ｔ２－ｔ１）分だけ遅れたものになる。

また、この動作において時刻ｔ２からタイムシフト再生が行われると、放送局から番組が放送されている間に、記録バッファ２０１４に一時記録され

ていたコンテンツは再生が終了するが、この再生終了時刻ｔ７から番組視聴終了時刻ｔ６までは、記録バッファ２０１４には、データの記録再生が行われるとともに、再生した番組データが視聴不可能な状態として保持されているか、消去されていることとなっている。

一方、時刻ｔ２を経過しても制御入力Ｉ／Ｆ２０１５にユーザからの入力が行われない場合は、記録バッファ２０１４に、設定された時間分のデータが全て記録される時刻ｔ３で、記録バッファ２０１４への一時記録動作は停止するとともに、強制的にタイムシフト再生が開始される。本実施の形態では、告知手段２０９１が告知を行った時刻ｔ２から５分経過した時刻ｔ３がこの時刻に相当する。この動作において、時刻ｔ３から、ポーズが開始された時刻ｔ１の差だけ遅れて、番組はタイムシフト再生されていることとなり、ユーザの番組視聴が終了する時刻ｔ５は、実際の放送の終了時刻ｔ４よりこの（ｔ３－ｔ１）分だけ遅れたものになる。また、この（ｔ３－ｔ１）分は、はじめに記録バッファ２０１４に設定された複製禁止コンテンツの記録時間と同一である。さらに、時刻ｔ３以降の放送は記録バッファ２０１４には記録されていない。したがって、強制的なタイムシフト再生の終了時刻ｔ８から、番組視聴終了時刻ｔ５までの間は、既に番組が放送終了した後に放送される別の番組をユーザは視聴することになるか、タイムシフト再生の終了時刻ｔ８がそのままユーザの視聴時刻となる。

つまり、時刻ｔ２を経過してもユーザからタイムシフト再生の入力が行なわれずに、一旦強制的にタイムシフト再生が開始されると、ユーザはポーズ前から視聴されていた番組を、ポーズ解除後は完全な形で視聴することができないことになる。

以上のように、本実施の形態によれば、ユーザが所望の時間に複製禁止コンテンツのタイムシフト再生を設定できるとともに、複製禁止コンテンツの著作権を保護するために、所定の時間が経過するまでに、ユーザにタイムシフト再生の完全な実行を促すことができる。

なお、上記の実施の形態においては、記録バッファ２０１４を用いた例にて説明を行ったが、記録バッファ２０１４の代わりに第１３の実施の形態のリングバッファ２０４４を用いても同様の効果が得られる。リングバッファ２０４４を用いた場合の動作は、図４２の一点鎖線部に示すように、時刻ｔ４からｔ３までの間、リングバッファである記録バッファには、データの上書き記録を続けながら同時に再生が行われることにより、バッファの設定時間分のタイムシフト再生が行われることとなる。ただし、時刻ｔ３で上書き動作を禁じるように設定した場合の動作は、上述した通常の記録バッファの強制的なタイムシフト再生実行の場合と同様となる。

また、本実施の形態の構成は、既に述べた第１４の実施の形態と組み合わせて用いてもよい。

さらに、上記の各実施の形態においては、本発明の記録装置と再生手段とを一体化した記録再生手段が記録バッファへの記録および再生を行うものとして説明を行ったが、本発明の構成はこれに限定するものではなく、記録を行う記録手段のみを備えたものとして、記録バッファ２０１４またはリングバッファ２０４４からデータ再生を行う手段は、外部装置として別途設けるようにしてもよい。

さらに、上記の各実施の形態において、複製禁止コンテンツの記録期間等は、時間情報として、コンテンツのＭＰＥＧストリーム内のＰＣＲパケット

をカウントする計測を行ったが、時間情報はこれに限定するものではなく、他の時間情報としてはＥＰＧを用いてもよく、取得したＥＰＧを参照して、別途設けたタイマによって絶対時刻測定を行うことにより、計測を行ってもよい。

さらに、この時間情報は、記録媒体２０１３にて計測されているものであってもよい。

さらに、この時間情報は、本発明の実施の形態の記録再生装置にＭＰＥＧストリームを入力するＳＴＢ等の機器内にて計測されているものであって、ＭＰＥＧストリームとともに入力するようにしてもよい。さらにこれら時間情報は、一時記録の対象となるコンテンツの放送開始時刻等を含むものであっても良い。

さらに、上記の各実施の形態において、複製禁止コンテンツは、一度の複製も許されないデータからなるものとして説明を行ったが、本発明の複製制限コンテンツはこれに限定するものではなく、一度だけ複製が許可されたデータからなるコンテンツを対象としてもよい。要するに、本発明は、複製が禁止または所定の制限が附されたデータに対してなら何でも用いることが可能である。

なお、本明細書には、上述した本発明の記録装置によってディスク記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第１

の情報を作成し、前記復号手段は、前記記録ユニット情報を用いて、前記第１の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記暗号化されたタイトルキーを前記デバイスユニークキーを用いて復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記復号手段は、前記タイトルキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて

復号し、前記復号手段は、前記タイトルキーを含む第３の情報を作成し、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手段は、前記第３の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記復号手段は、前記コピー許諾情報を用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて復号し、前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかをを含む第２の情報を作成し、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手

段は、前記第２の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記コピー許諾情報を再生するよう前記記録手段を制御し、前記復号手段は、前記データを前記再生されたコピー許諾情報を用いて復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラム及び／またはデータが前記コンピュータと協動して前記機能を実行する媒体に関する発明も記載されている。

さらに、本明細書には、上述した本発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータである情報集合体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラム及び／またはデータが前記コンピュータと協動して前記機能を実行する情報集合体に関する発明も記載されている。

さらに、データとは、データ構造、データフォーマット、データの種類などを含む。

さらに、媒体とは、ＲＯＭ等の記録媒体、インターネット等の伝送媒体、

光・電波・音波等の伝送媒体を含む。

さらに、担持した媒体とは、例えば、プログラム及び／またはデータを記録した記録媒体、やプログラム及び／またはデータを伝送する伝送媒体等を含む。

さらに、コンピュータにより処理可能とは、例えば、ＲＯＭなどの記録媒体の場合であれば、コンピュータにより読みとり可能であることであり、伝送媒体の場合であれば、伝送対象となるプログラム及び／またはデータが伝送の結果として、コンピュータにより取り扱えることであることを含む。

さらに、情報集合体とは、例えば、プログラム及び／またはデータ等のソフトウエアを含むものである。

さらに、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

産業上の利用可能性

以上説明したところから明らかなように、本発明は、著作権保護が必要なデータを記録する場合及び／または著作権保護が必要なデータを再生する場合に著作権を保護することが出来る記録装置及び再生装置とを提供することが出来る。

また、本発明は、著作権を保護しつつ、コピーが禁止されているデータを他の記録媒体に移動させるまたは複写するデータ処理装置と、そのデータ処理装置からのデータを記録媒体に記録し、または記録するとともに再生する記録再生装置と、著作権を保護してデータをバックアップしておく暗号化データ復号記録装置システムおよびそのシステムを構成する復号記録装置、記

録装置と、著作権を保護してデータを送信するデータ送信装置とを提供することができる。

また、本発明は、複製が禁じられた放送番組等を、著作権侵害を回避するようにしてタイムシフト再生を行うことが出来る記録装置及び記録再生装置とを提供することが出来る。

請　求　の　範　囲

1．　インターフェースから送られてくるデータを暗号化する暗号化手段と、

前記暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置。

2．　前記暗号化手段は、記録装置自らに割り付けられた固有の数値及び／または記号であるデバイスユニークキーを用いて、前記データを暗号化することを特徴とする請求項１記載の記録装置。

3．　前記暗号化手段は、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記データを暗号化することを特徴とする請求項１または２に記載の記録装置。

4．　前記記録ユニット情報を用いて、前記データを暗号化するとは、前記記録ユニット情報に基づいて得られたキーで前記データを暗号化することであることを特徴とする請求項３記載の記録装置。

5．　少なくとも前記記録ブロックに記録される前記暗号化されたデータ及び前記暗号化されたデータに付加された付加情報は、すべての部分が暗号化されて前記記録手段に記録されることを特徴とする請求項３または４に記載の記録装置。

6．　前記データには、コピー許諾情報が付加されており、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記デバイスユニークキーと前記コピー許諾情報の少なく

ともいずれかを含む第１の情報を作成し、

前記記録ユニット情報を用いて、前記暗号化手段は、前記第１の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項３～５のいずれかに記載の記録装置。

７．　前記データには、前記データに固有の数値及び／または記号であるタイトルキーが割り付けられており、

前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段に記録するように前記記録手段を制御することを特徴とする請求項２記載の記録装置。

８．　前記暗号化手段は、前記タイトルキーを用いて前記データを暗号化することを特徴とする請求項７記載の記録装置。

９．　前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーを含む第３の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第３の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項８記載の記録装置。

１０．　前記データには、コピー許諾情報が付加されており、

前記暗号化手段は、前記コピー許諾情報をも用いて、前記データを暗号化することを特徴とする請求項８記載の記録装置。

１１．　前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかを含む第２の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第２の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項１０記載の記録装置。

１２．　前記暗号化手段は、コピー許諾情報が付加され、インターフェースから送られてくるデータを前記コピー許諾情報を用いて暗号化し、

前記制御手段は、前記記録手段が前記データを記録する前及び／または前記データを記録した後に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項１記載の記録装置。

１３．　前記制御手段は、少なくとも前記記録手段が前記データを記録する前に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項１２記載の記録装置。

１４．　前記制御手段は、前記記録手段が前記データを記録した後のみに、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項１２記載の記録装置。

１５．　インターフェースから送られてくる暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置。

１６．　請求項１記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備えたことを特徴とする再生装置。

１７．　請求項２記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記デバイスユニークキーを用いて前記再生されたデータを

復号することを特徴とする再生装置。

１８．　請求項３記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報を用いて前記再生されたデータを復号することを特徴とする再生装置。

１９．　請求項４記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報に基づいて得られたキーで前記再生されたデータを復号することを特徴とする再生装置。

２０．　請求項１４記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記データの記録時に、前記コピー許諾情報が前記記録手段に正常に記録出来なかった場合、前記復号手段は、前記コピー許諾情報が各値を取ると仮定して前記暗号化されたデータの全部または一部の復号を試行し、

前記試行した結果、前記再生されたデータが正常に復号出来た場合の前記コピー許諾情報の値を用いて前記再生されたデータを復号することを特徴とする再生装置。

２１．　請求項１５記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段とを備え、

前記再生されたデータは、インターフェースに送られることを特徴とする再生装置。

２２．　前記インターフェース、前記暗号化手段及び前記制御手段が、同一プリント基板上に一体化して配設されていることを特徴とする請求項１～１４のいずれかに記載の記録装置。

２３．　前記インターフェース、前記暗号化手段及び前記制御手段は、１チップ化されていることを特徴とする請求項２２記載の記録装置。

２４．　前記インターフェース、前記復号手段及び前記制御手段が同一プリント基板上に一体化して配設されていることを特徴とする請求項１６～２０のいずれかに記載の再生装置。

２５．　前記インターフェース、前記復号手段及び前記制御手段は、１チップ化されていることを特徴とする請求項２４記載の再生装置。

２６．　第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする請求項２２記載の記録装置。

２７．　第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする請求項２４記載の再生装置。

２８．　第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とす

る請求項２２記載の記録装置。

２９．　第３者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする請求項２４記載の再生装置。

３０．　前記デバイスユニークキーは、外部の機器がアクセスすることが出来ないことを特徴とする請求項２～１１のいずれかに記載の記録装置。

３１．　前記コピー許諾情報は、前記記録手段のユーザから直接アクセスできないシステム領域に記録されることを特徴とする請求項６、１０、１１、１２、１３、１４のいずれかに記載の記録装置。

３２．　前記インターフェースから送られてくるデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止（ｃｏｐｙ　ｎｅｖｅｒ）を表す場合であっても、前記記録手段が前記データを記録するように制御することが出来ることを特徴とする請求項１～１５、２２、２３、２６、２８、３０、３１のいずれかに記載の記録装置。

３３．　前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする請求項３２記載の記録装置。

３４．　前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする請求項３２記載の記録装置。

３５．　前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止（ｃｏｐｙ　ｎｅｖｅｒ）を表す場合、前記再生手段が前記データを少

なくとも１回再生するよう制御することを特徴とする請求項１６～２１、２４、２５、２７、２９のいずれかに記載の再生装置。

３６．　前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする請求項３５記載の再生装置。

３７．　前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする請求項３５記載の再生装置。

３８．　前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、１回だけ複製することを許可（ｃｏｐｙ　ｏｎｃｅ）することを表す場合、前記記録手段により１回複製された後の前記データの前記コピー許諾情報が、再び１回だけ複製することを許可（ｃｏｐｙ　ｏｎｃｅ）することを表すようにして、前記再生手段が前記データを１回だけ複製出力するよう制御することを特徴とする請求項１６～２１、２４、２５、２７、２９のいずれかに記載の再生装置。

３９．　前記所定の条件とは、前記再生手段が前記データを複製出力した所定の時間後に、前記データもしくは前記データの暗号化に用いたキーを消去する場合であるであることを特徴とする請求項３８記載の再生装置。

４０．　前記所定の条件とは、１回だけ複製出力された前記データの記録先がバックアップ用として前記データを記録する装置である場合であることを特徴とする請求項３８記載の再生装置。

４１．　前記記録先でバックアップ用として記録された前記データは、前記記録先では再生不可であることを特徴とする請求項４０記載の再生装置。

４２．　前記記録先でバックアップ用として記録された前記データは、元の再

生装置に戻さない限り再生不可であることを特徴とする請求項４０記載の再生装置。

４３．　前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報の値に関係なく前記データを暗号化することを特徴とする請求項１～１４、２２、２３、２６、３０～３４のいずれかに記載の記録装置。

４４．　前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報が自由に複製してもよいこと（Ｃｏｐｙ　ｆｒｅｅ）を表す場合、前記データを暗号化せず、

前記制御手段は、前記記録手段が前記暗号化されていないデータを記録するように制御することを特徴とする請求項１～１４、２２、２３、２６、３０～３４のいずれかに記載の記録装置。

４５．　データが記録される記録媒体に記録されているデータを他の記録装置へ移動させる移動手段を少なくとも備えたデータ処理装置であって、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

ことを特徴とするデータ処理装置。

４６．　データが記録される記録媒体に記録されているデータを他の記録装置に複写する複写手段を少なくとも備えたデータ処理装置であって、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化

されている

ことを特徴とするデータ処理装置。

４７．　前記コピー禁止データを前記暗号化鍵で暗号化する暗号化手段をさらに備えたことを特徴とする請求項４５または４６に記載のデータ処理装置。

４８．　前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する再生手段をさらに備えたことを特徴とする請求項４５～４７のいずれかに記載のデータ処理装置。

４９．　前記再生手段は、ユーザが視聴するさいに必要な速度で前記コピー禁止データを再生する手段であって、

前記他の記録装置から前記ユーザが視聴するさいに必要な速度よりも速い速度で、前記暗号化鍵で暗号化されている前記コピー禁止データが送信されてきた場合、送信されてきた前記コピー禁止データを、前記ユーザが視聴するさいに必要な速度よりも速い速度で格納する格納手段をさらに備え、

前記再生手段は、前記格納手段が前記他の記録装置からの前記コピー禁止データを格納するさいに、前記格納手段に格納された前記コピー禁止データもしくは、予め前記格納手段に格納されたデータを再生することができる

ことを特徴とする請求項４８に記載のデータ処理装置。

５０．　前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記第２の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項４５～４９のいずれかに記載のデータ処理装置。

５１．　前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項４５～４９のいずれかに記載のデータ処理装置。

５２．　前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを１回だけコピー可能なデータとして出力することを特徴とする請求項４５～５１のいずれかに記載のデータ処理装置。

５３．　請求項４５～４７のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段を備えたことを特徴とする記録再生装置。

５４．　請求項４８記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理

装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置。

５５．　請求項５０または５１に記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置。

５６．　請求項４５、４６、４７、５０、５１のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する解読再生手段とを備えた

ことを特徴とする記録再生装置。

５７．　前記暗号化鍵が記録されている暗号化鍵記録媒体を再生する鍵再生手段と、

前記鍵再生手段が再生した前記暗号化鍵を記憶する鍵記憶手段とをさらに備え、

前記解読再生手段は、前記鍵記憶手段が記憶している前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする請求項５６記載の記録再生装置。

５８．　前記データ処理装置から送信されてきた前記暗号化鍵を受信する受信手段をさらに備え、

前記解読再生手段は、前記受信手段によって受信された前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする請求項５６記載の記録再生装置。

５９．　データが記録される記録媒体に記録されているデータを、他の記録装置へ、その他の記録装置において解読される形式のデータとして移動させる移動手段を少なくとも備え、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置。

６０．　データが記録される記録媒体に記録されているデータを、他の記録装置に、その他の記録装置において解読される形式のデータとして複写する複写手段を少なくとも備え、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置。

６１．　前記他の記録装置において解読される形式のデータとは、平文データ、または前記他の記録装置固有の鍵で暗号化されたデータ、または前記他の記録装置における第２の記録媒体に付されている鍵で暗号化されたデータを意味することを特徴とする請求項５９または６０に記載のデータ処理装置。

６２．　前記他の記録装置において解読される形式のデータが、さらに、

前記他の記録装置において用いられるフォーマットのデータでもあることを特徴とする請求項６１記載のデータ処理装置。

６３．　前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記第２の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項５９～６２のいずれかに記載のデータ処理装置。

６４．　前記第２の記録媒体に、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であることを示す鍵が付されている場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記第２の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項６３記載のデータ処理装置。

６５．　前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項５９～６２のいずれかに記載のデータ処理装置。

６６．　前記他の記録装置が、前記データ処理装置に対応する装置であることを示す鍵を有している場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項６５記載のデータ処理装置。

６７．　前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを１回だけコピー可能なデータとして出力することを特徴とする請求項５９～６６のいずれかに記載のデータ処理装置。

６８．　請求項５９または６０に記載のデータ処理装置からの前記コピー禁止データを第２の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが平文データであり、

前記コピー禁止データを、前記第２の記録媒体に付されている暗号化鍵を用いて、または前記記録再生装置固有の暗号化鍵を用いて暗号化する暗号化手段と、

前記暗号化手段によって暗号化された前記コピー禁止データを前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置。

６９．　請求項５９または６０に記載のデータ処理装置からの前記コピー禁止データを第２の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが前記記録再生装置固有の鍵で暗号化されたデータ、または前記第２の記録媒体に付されている鍵で暗号化されたデータであり、

前記暗号化された前記コピー禁止データを前記第２の記録媒体に記録する記録手段と、

前記第２の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置。

７０．　前記移動手段が前記データの移動を行ったさい、または前記複写手段が前記データの複写を行ったさい、前記データの移動または複写に対する課金情報を、前記データ処理装置を管理する管理装置に送信する課金情報送信手段をさらに備えたことを特徴とする請求項４５、４６、４７、４８、４９、５０、５１、５２、５９、６０、６１、６２、６３、６４、６５、６６、６７のいずれかに記載のデータ処理装置。

７１．　前記データ処理装置と前記他の記録装置とが接続されたインタフェースに、少なくとも前記コピー禁止データの移動または複写に対して課金

能力を有する管理装置が接続されていることが確認されたときに、前記移動手段または前記複写手段は、前記コピー禁止データを前記他の記録装置に移動させるまたは複写することを特徴とする請求項４５、４６、４７、４８、４９、５０、５１、５２、５９、６０、６１、６２、６３、６４、６５、６６、６７のいずれかに記載のデータ処理装置。

７２．　同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置と、

それら複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを有する復号記録装置とを備えた

ことを特徴とする暗号化データ復号記録装置システム。

７３．　同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、

前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを備えた

ことを特徴とする復号記録装置。

７４．　同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置のうちの一つの記録装置であって、

前記暗号化された前記コピー禁止データを記録する記録手段と、その記録手段に記録されている前記暗号化されたコピー禁止データを出力する出力手

段とを備え、

その出力手段から出力される前記暗号化されたコピー禁止データは、その暗号化されたコピー禁止データを復号する復号手段を少なくとも有する復号記録装置においてのみ復号されるデータである

ことを特徴とする記録装置。

７５．　複数個のデータで構成されているストリームを送信する送信手段を備え、

前記ストリームの、または前記ストリームを構成する各ブロック内の、複数個の前記データそれぞれは、そのデータの時間上一つ手前のデータが再生されないと再生されないデータであって、

前記送信手段は、前記ストリームの、または前記ストリームを構成する各ブロック内の、前記複数個のデータの時間的に最後尾から先頭側の順に、前記各データを送信する

ことを特徴とするデータ送信装置。

７６．　複製が禁止または制限されるよう設定されているデータからなる複製制限コンテンツをタイムシフト再生可能にするための記録装置であって、

所定の容量分、前記複製制限コンテンツの記録が可能な記録媒体と、

前記記録媒体に対しデータの記録を行う記録手段とを備え、

前記記録手段は、前記複製制限コンテンツを前記記録媒体に記録するとともに、前記複製制限コンテンツの記録を開始した時刻から、所定の時間が経過した後、前記記録媒体に記録された前記複製制限コンテンツのデータを、視聴することが不可能な状態にすることを特徴とする記録装置。

７７．　前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去することにより実現することを特徴とする請求項７６記載の記録装置。

７８．　前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去しないことにより実現することを特徴とする請求項７６記載の記録装置。

７９．　前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを再生不可能にすることにより実現することを特徴とする請求項７６記載の記録装置。

８０．　前記視聴することが不可能な状態を、再生後の前記複製制限コンテンツのデータを暗号化することにより実現することを特徴とする請求項７９記載の記録装置。

８１．　前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、前記複製制限コンテンツに関連した判別情報を参照することにより定められることを特徴とする請求項７６～８０のいずれかに記載の記録装置。

８２．　前記記録手段は、前記判別情報を用いて、前記複製制限コンテンツと他のコンテンツとを分別して記録を行うことを特徴とする請求項８１記載の記録装置。

８３．　前記判別情報は、前記複製制限コンテンツのデータ列に含まれる著作権情報であることを特徴とする請求項８１記載の記録装置。

８４．　前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、外部からの入力に基づき定められることを特徴とする請求項７６

～８２のいずれかに記載の記録装置。

８５． 前記記録媒体は、前記複製制限コンテンツの一時記録を行うための記録バッファを有することを特徴とする請求項７６～８０のいずれかに記載の記録装置。

８６． 前記記録用バッファは、同一領域に上書き記録を繰り返すことにより一定量のデータを記録することが可能なリングバッファであることを特徴とする請求項８５記載の記録装置。

８７． 請求項７６～８５のいずれかに記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置。

８８． 請求項８６記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置。

８９． 前記リングバッファに上書き記録が行われている状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上にて、最も古いデータが記録されている位置から該データの再生を行うことを特徴とする請求項８８記載の記録再生装置。

９０．　前記リングバッファに上書き記録が行われていない状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上の記録開始位置から前記データの再生を行うことを特徴とする請求項８９記載の記録再生装置。

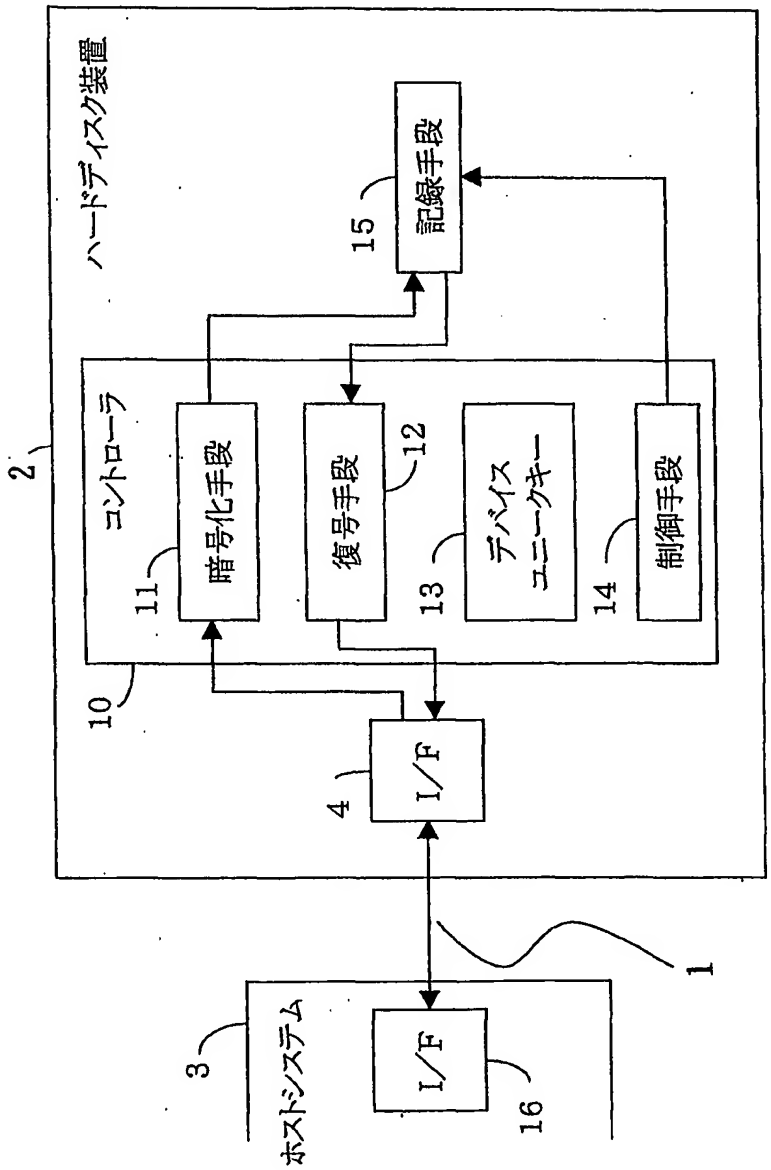
９１．　前記記録装置は、前記記録媒体に記録された複製制限コンテンツが、前記所定の待機時間内に再生されない場合、該複製制限コンテンツの記録動作を停止することを特徴とする請求項８７または８８に記載の記録再生装置。

９２．　前記所定の時間または前記所定の待機時間のいずれかに基づき、前記記録装置または再生手段の動作内容をあらかじめ告知する告知手段をさらに備えたことを特徴とする請求項８７または８８に記載の記録再生装置。

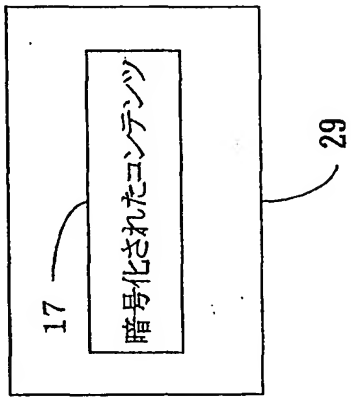
９３．　前記記録手段は、前記所定の時間を含む時間情報を、計測できることを特徴とする請求項７６記載の記録装置。

９４．　前記複製制限コンテンツは、前記所定の時間を含む時間情報を含んでいることを特徴とする請求項７６記載の記録装置。

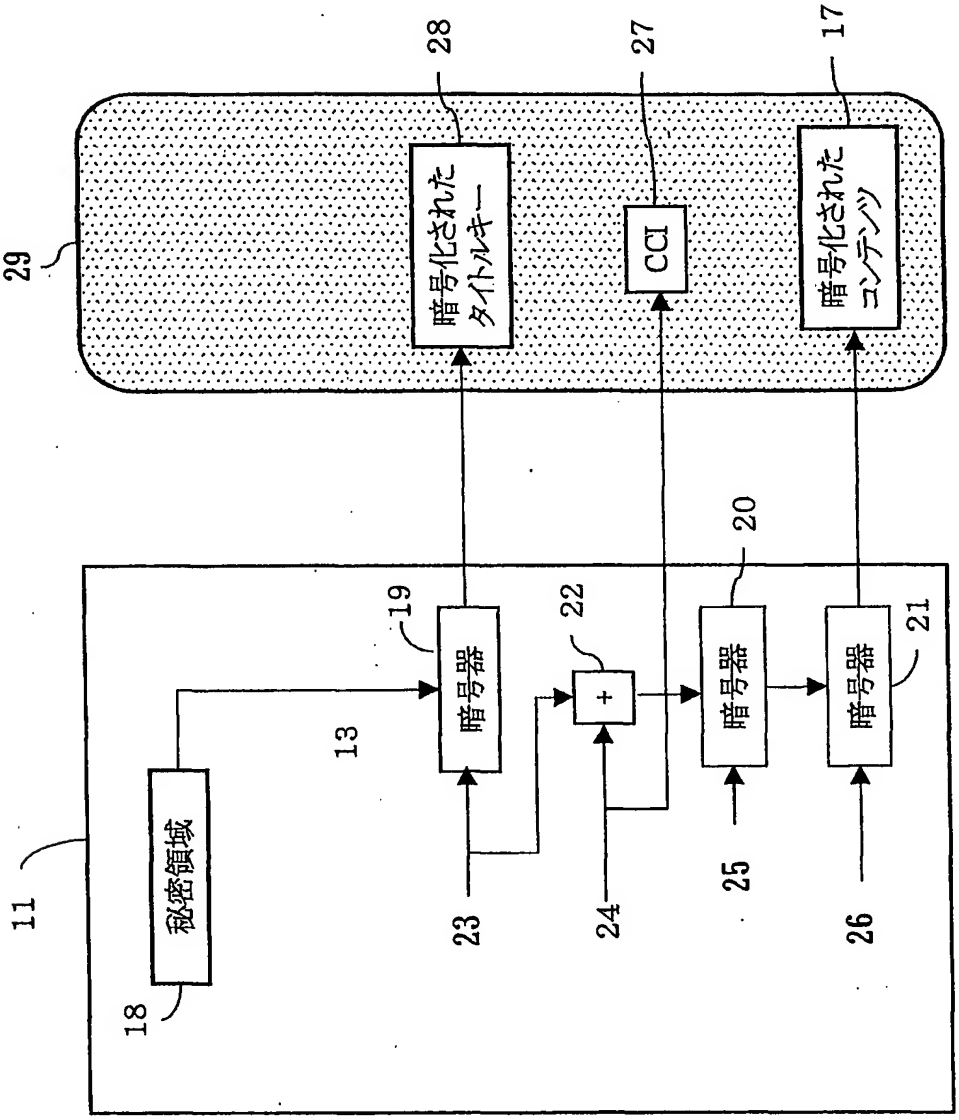
９５．　前記所定の時間を含む時間情報を、前記複製制限コンテンツとは独立して外部から取得することを特徴とする請求項７６記載の記録装置。


ハードディスク装置
2
コントローラ
10
暗号化手段
11
復号手段
12
デバイス
ユニークキー
13
制御手段
14
記録手段
15
I/F
4
1
ホストシステム
3
I/F
16

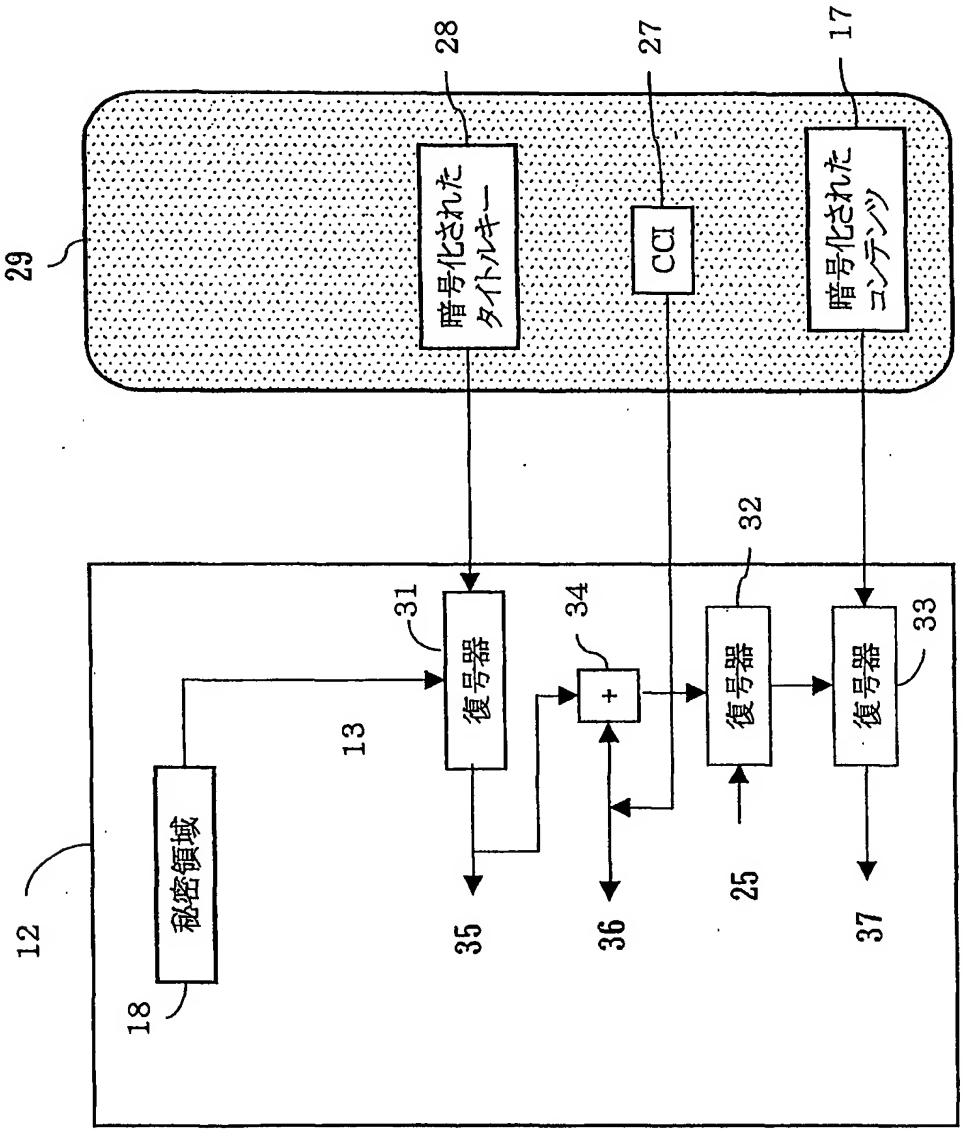
第1図


暗号化されたコンテンツ
17
29

第2図

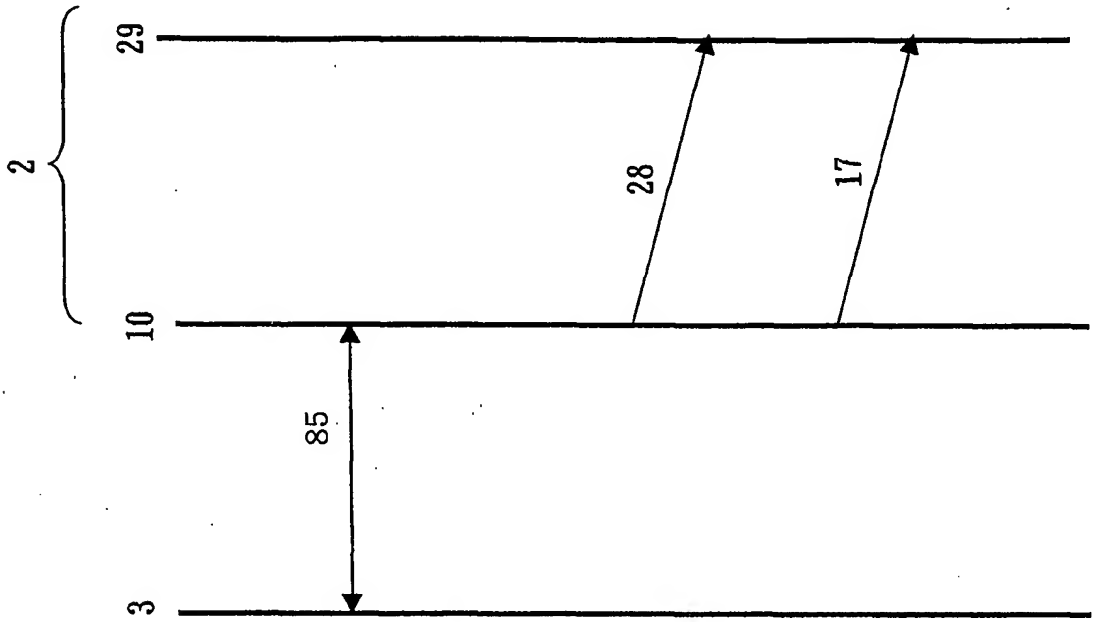

29
28
暗号化された
タイトルキー
27
CCI
17
暗号化された
コンテンツ
11
秘密領域
18
13
19
暗号器
22
+
20
暗号器
21
暗号器
23
24
25
26

第3図

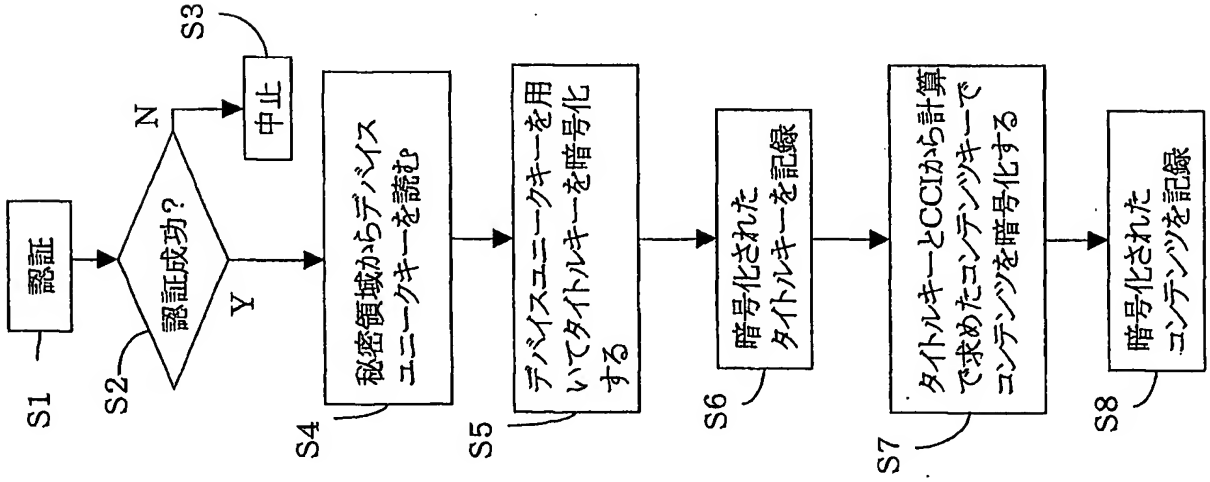

29
28
暗号化されたタイトルキー
27
CCI
17
暗号化されたコンテンツ
12
秘密領域
18
13
31
復号器
34
+
32
復号器
33
復号器
35
36
25
37

第４図

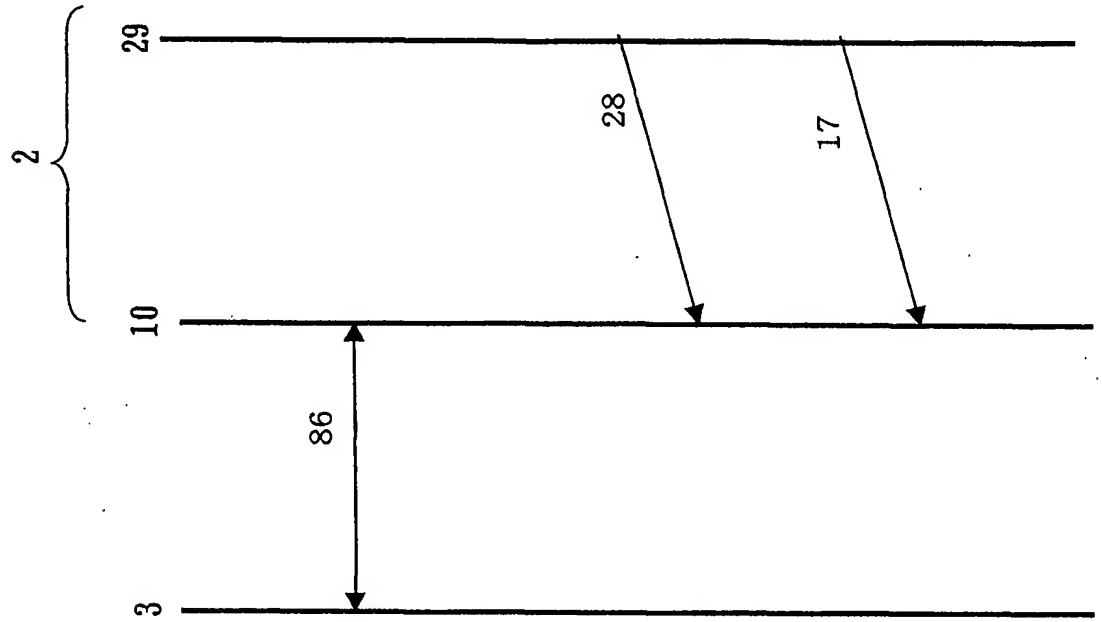
第5（b）図


2
29
28
17
10
85
3

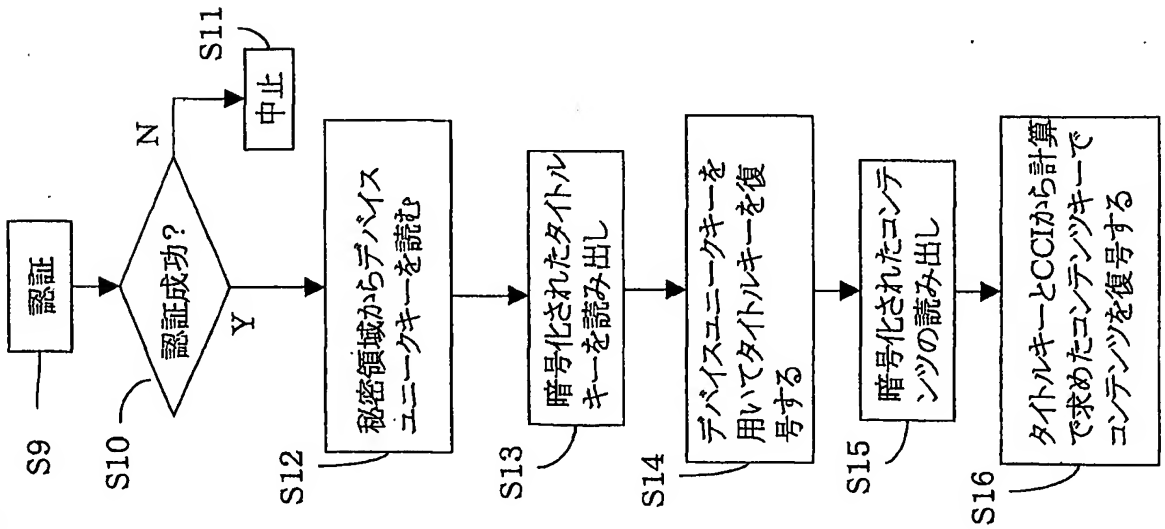
第5（a）図


認証
S1
認証成功?
S2
N
S3
中止
Y
秘密領域からデバイスユニークキーを読む
S4
デバイスユニークキーを用いてタイトルキーを暗号化する
S5
暗号化されたタイトルキーを記録
S6
タイトルキーとCCIから計算で求めたコンテンツキーでコンテンツを暗号化する
S7
暗号化されたコンテンツを記録
S8

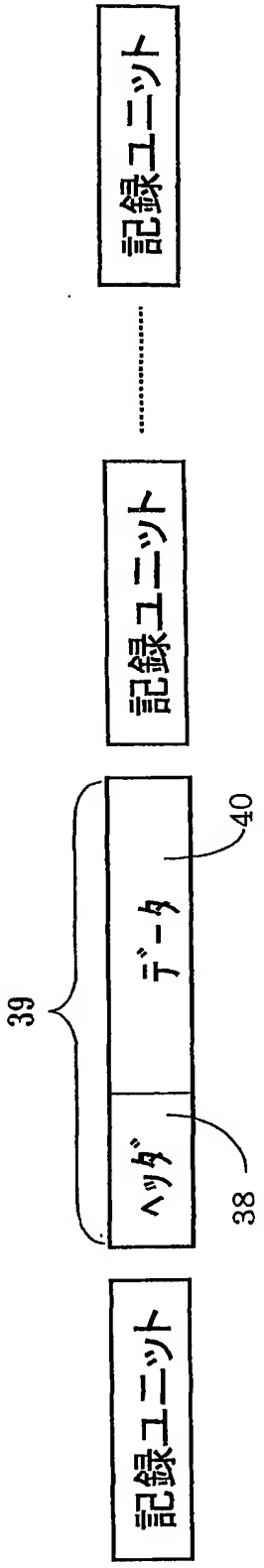
第６（ｂ）図


2
29
28
17
10
86
3

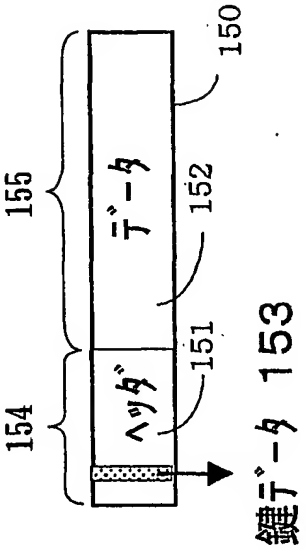
第６（ａ）図


S9
認証
S10
認証成功?
N
S11
中止
Y
S12
秘密領域からデバイスユニークキーを読み
S13
暗号化されたタイトルキーを読み出し
S14
デバイスユニークキーを用いてタイトルキーを復号する
S15
暗号化されたコンテンツの読み出し
S16
タイトルキーとCCIから計算で求めたコンテンツキーでコンテンツを復号する

第7（a）図


記録ユニット
ﾍｯﾀﾞ
ﾃﾞｰﾀ
記録ユニット
記録ユニット
39
40
38

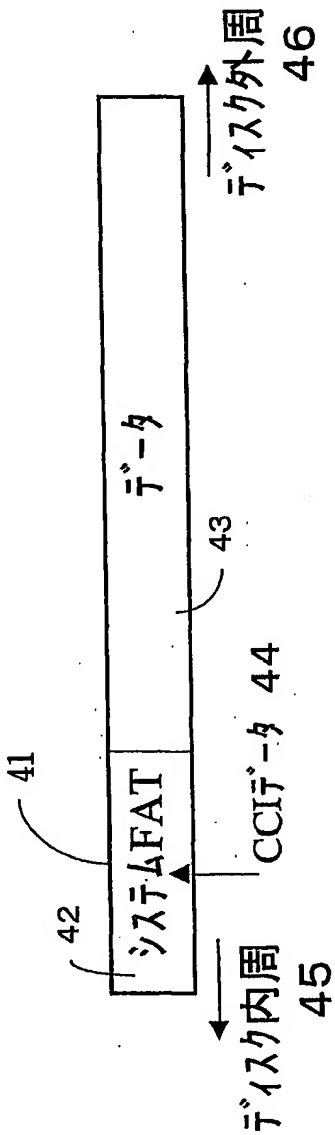
第7（b）図

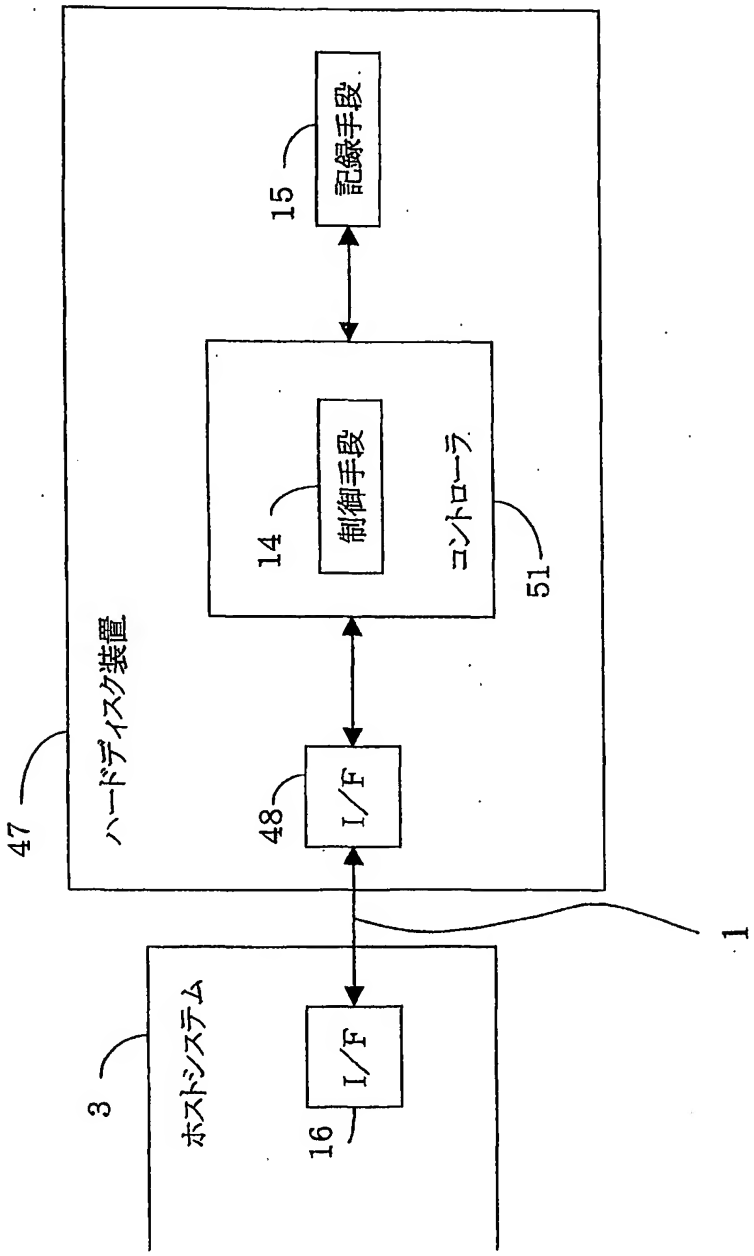

ﾍｯﾀﾞ
ﾃﾞｰﾀ
鍵ﾃﾞｰﾀ 153
154
155
150
151
152

第8図

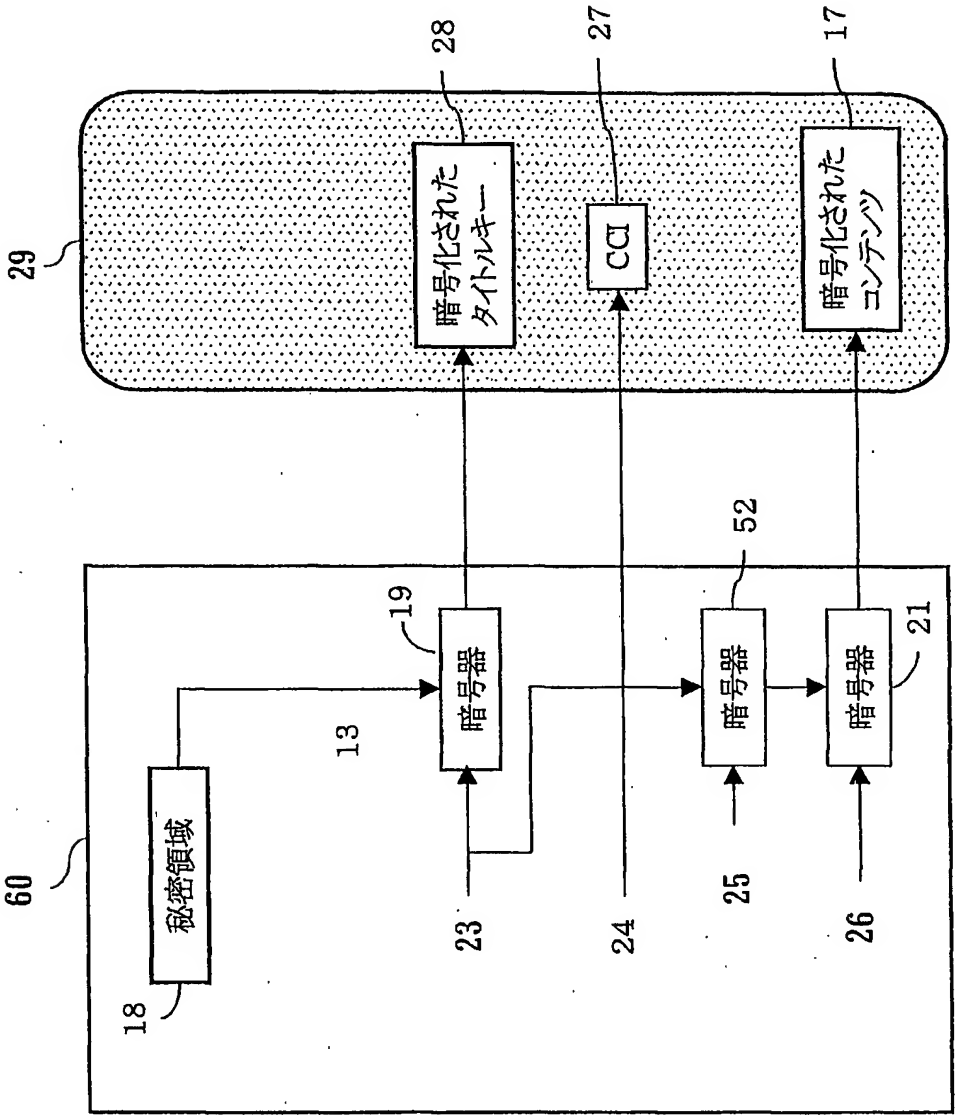
CCIの値	意味
11	Copy Never
10	Copy Once
01	No More Copy
00	Copy Free

第9図

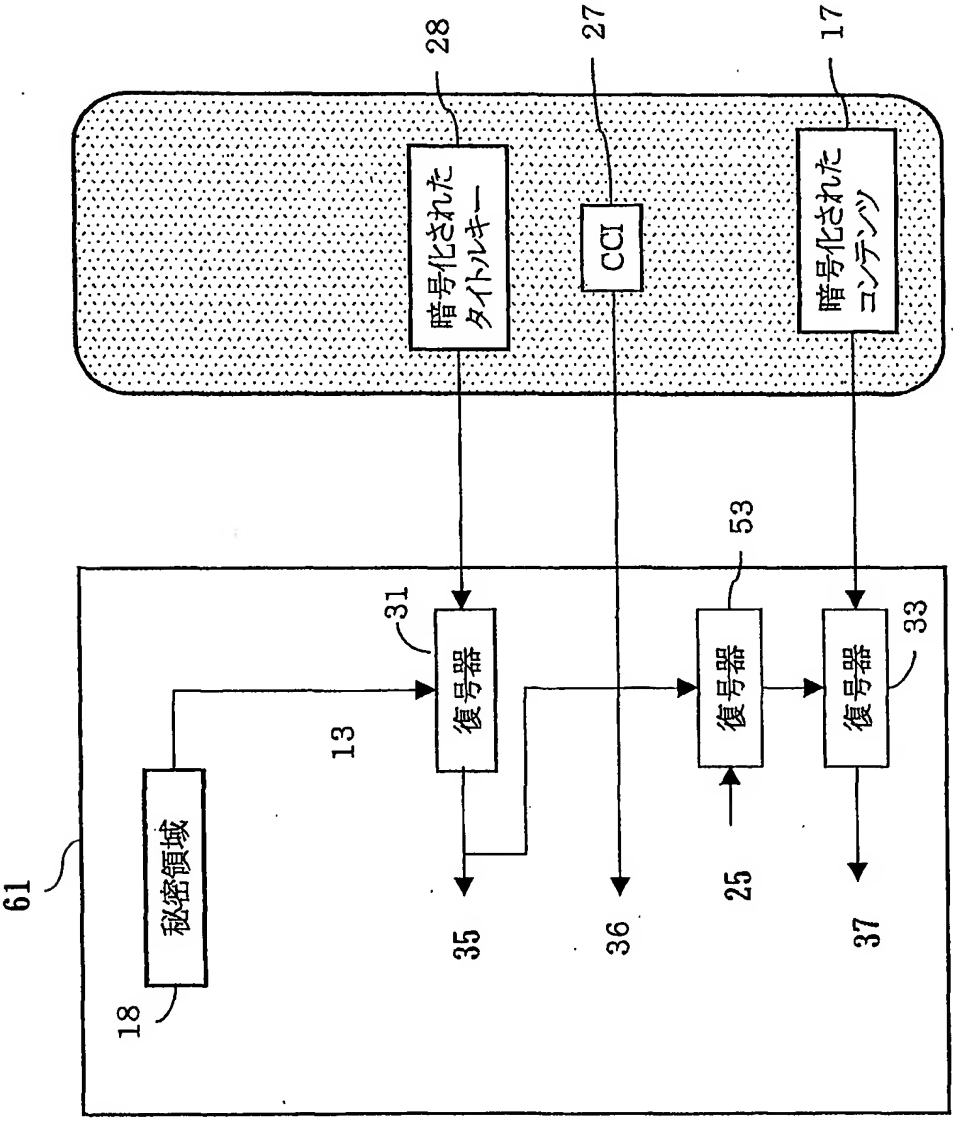




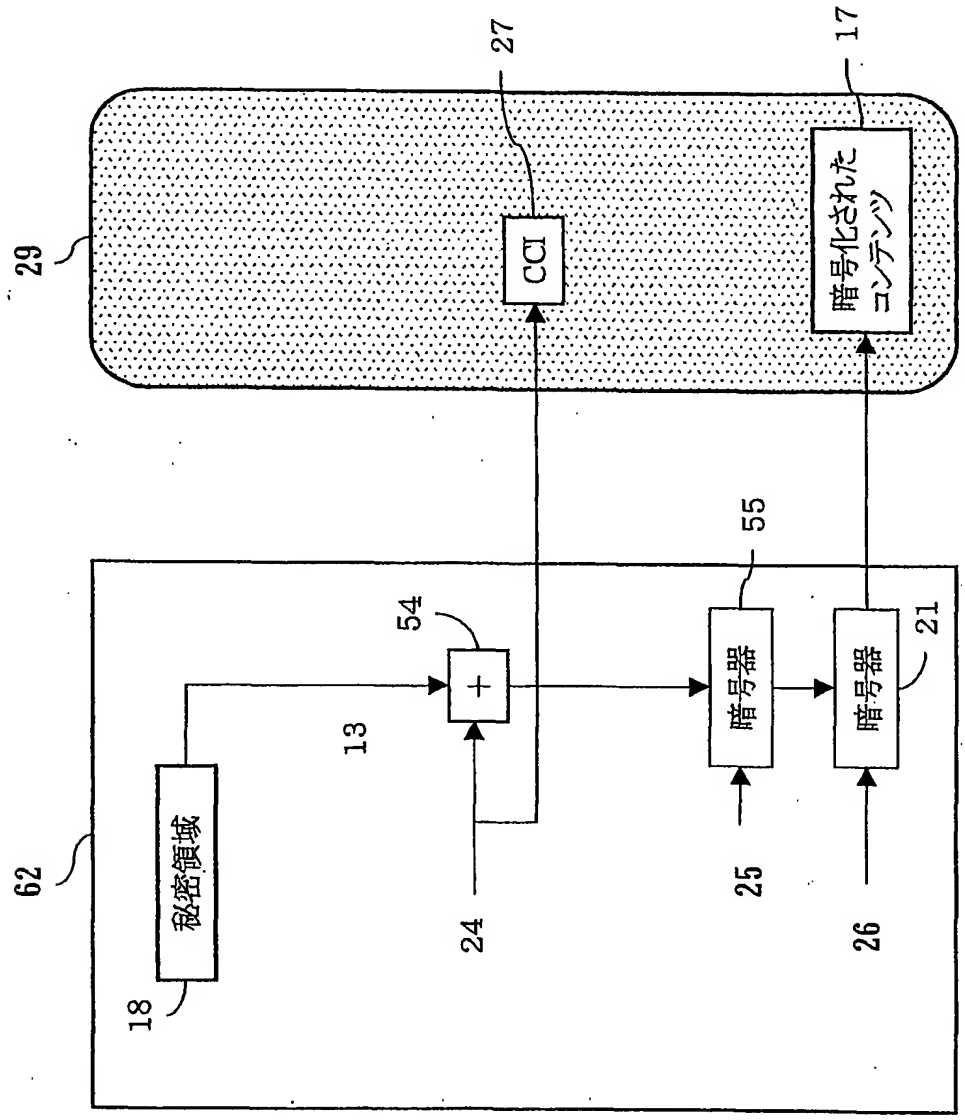
第１０図


29
28
暗号化された
タイトルキー
27
CCI
17
暗号化された
コンテンツ
60
秘密領域
18
13
19
暗号器
52
暗号器
21
暗号器
23
24
25
26

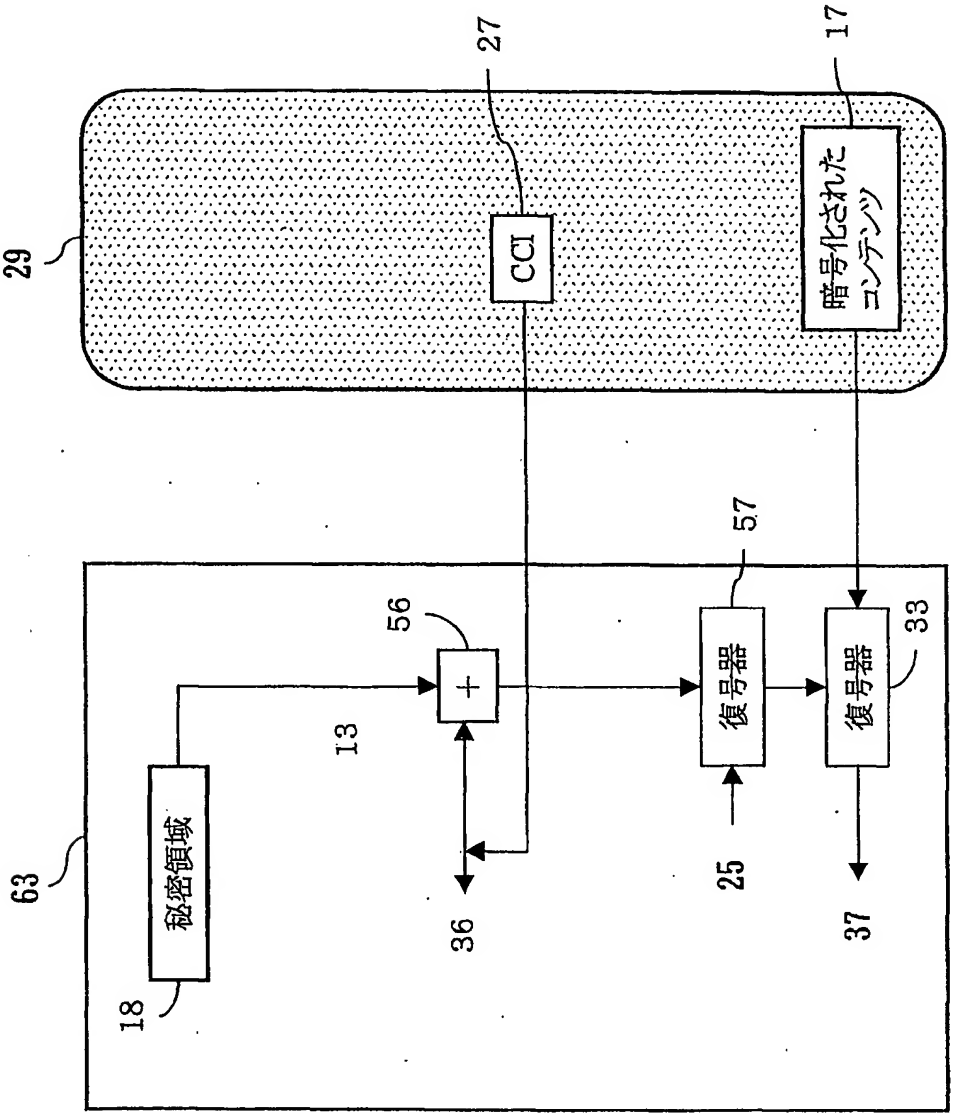
第１１図


28
27
17
暗号化されたタイトルキー
CCI
暗号化されたコンテンツ
53
31
33
復号器
復号器
復号器
13
61
秘密領域
18
35
36
25
37

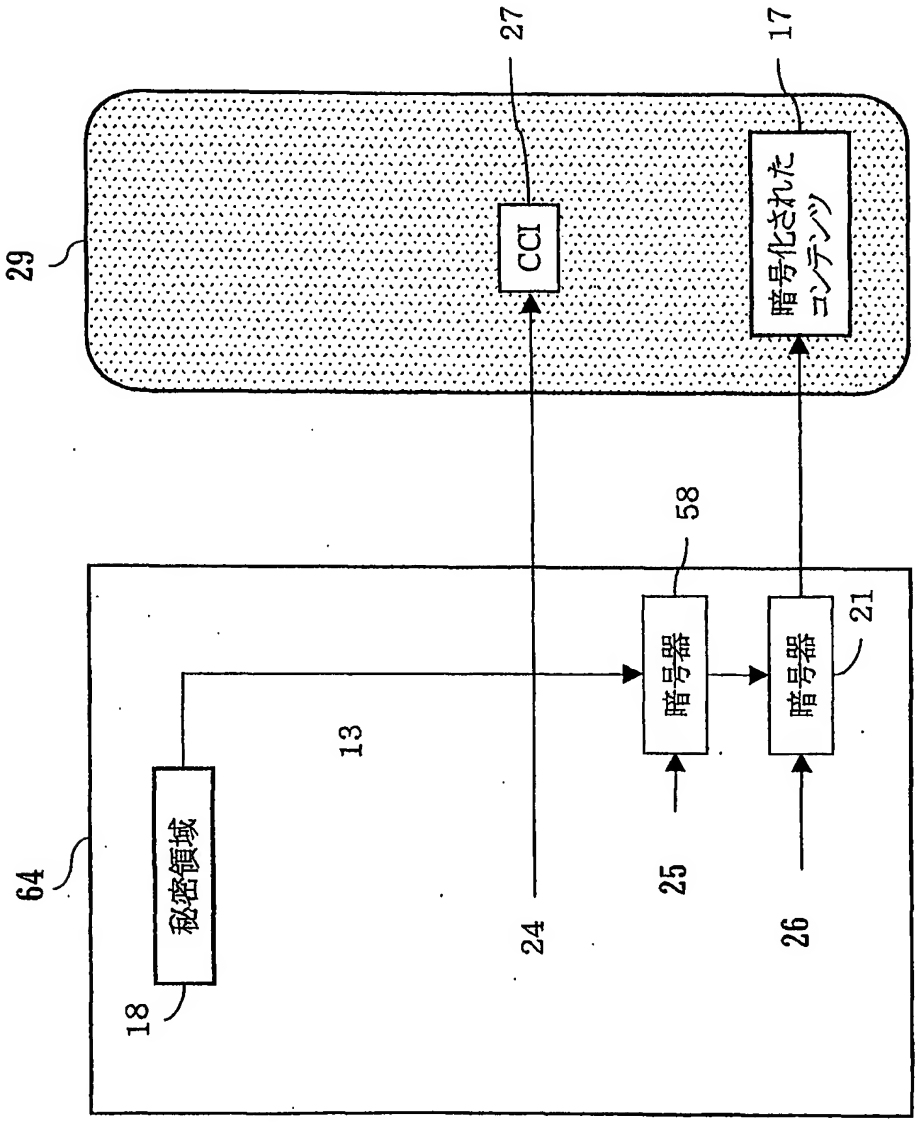
第１２図



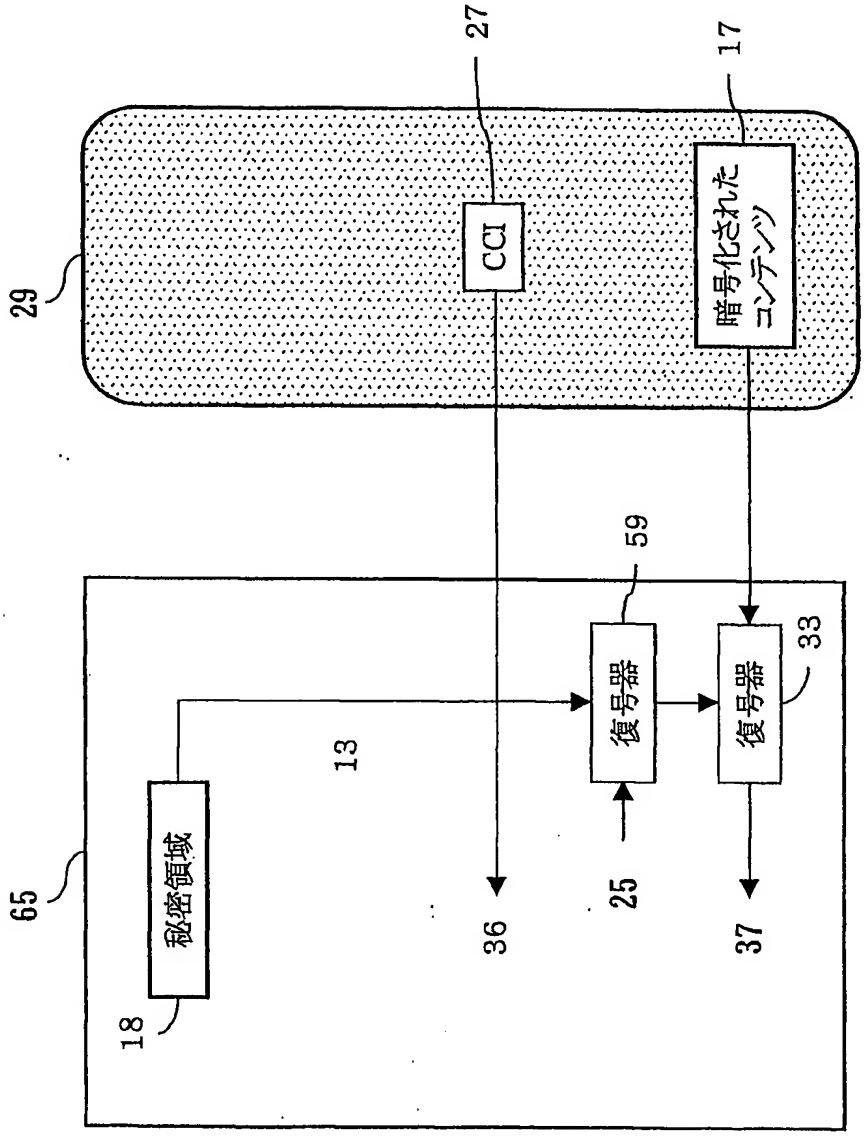
第１３図



第14図

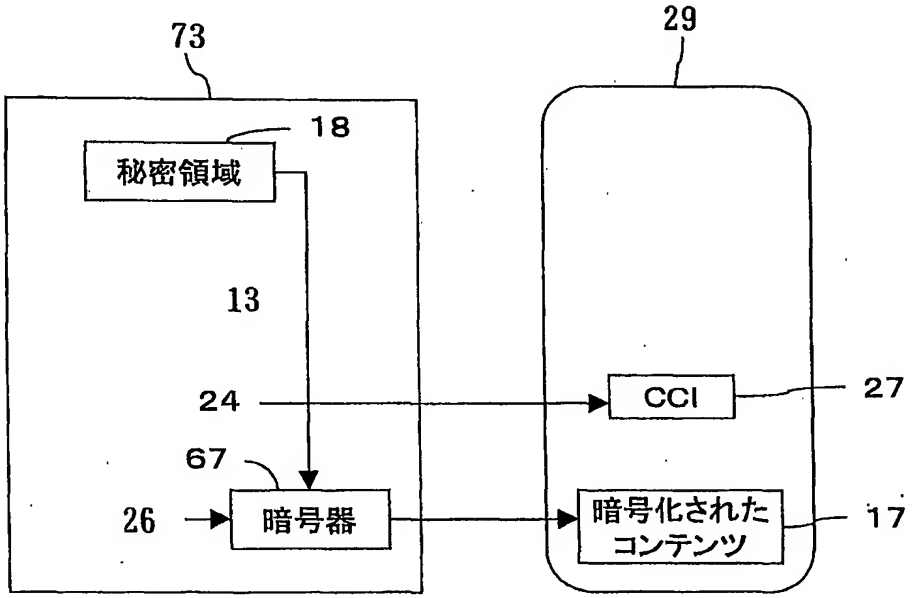


第15図

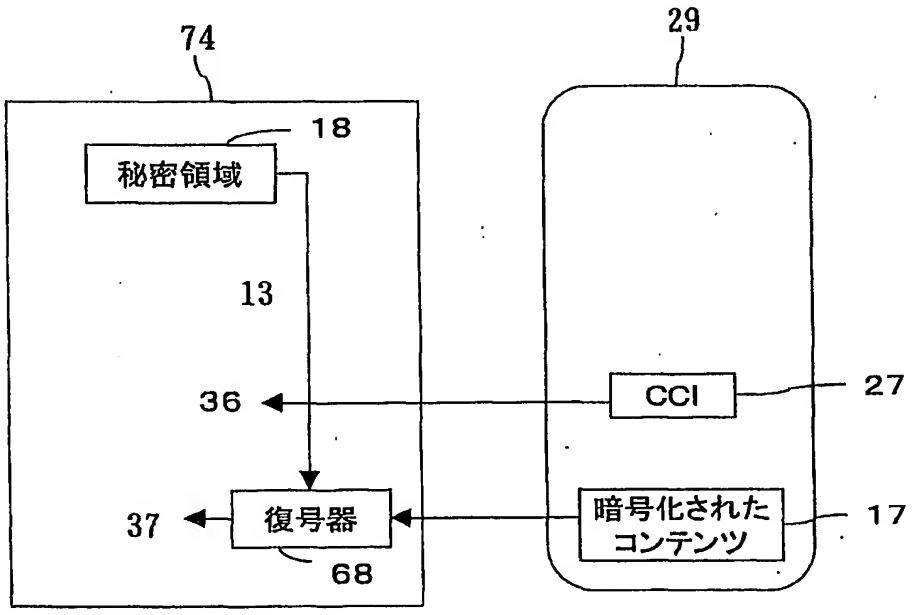


第16図

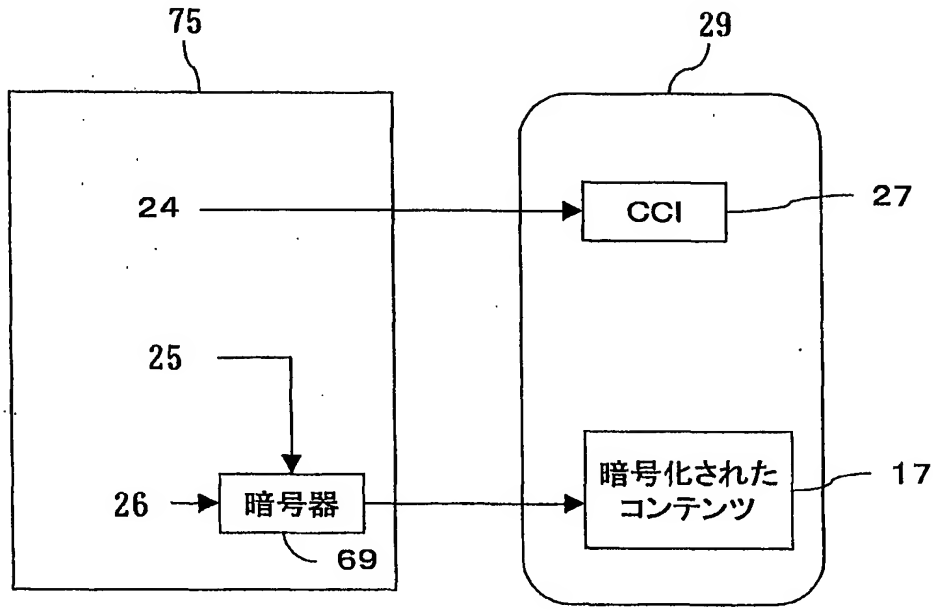
第１７（ａ）図


73
29
18
秘密領域
13
24
CCI
27
67
26
暗号器
暗号化された
コンテンツ
17

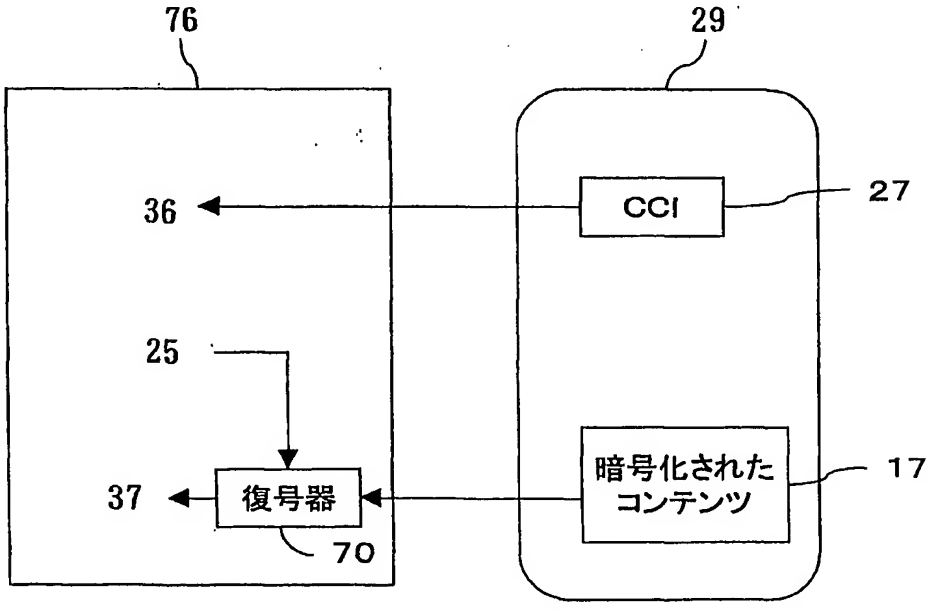
第１７（ｂ）図


74
29
18
秘密領域
13
36
CCI
27
37
復号器
68
暗号化された
コンテンツ
17

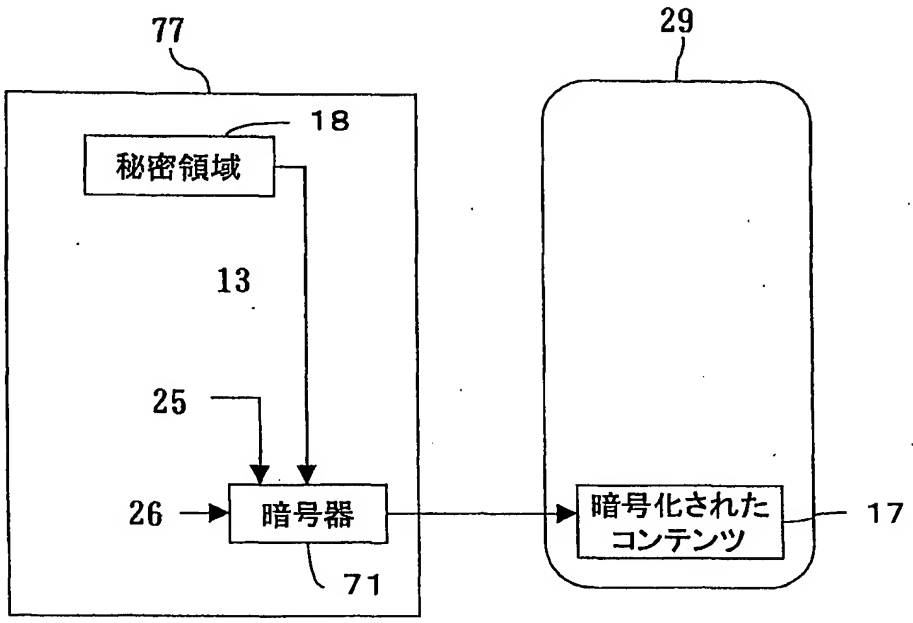
第１８（ａ）図


75
29
24
CCI
27
25
暗号器
26
69
暗号化された
コンテンツ
17

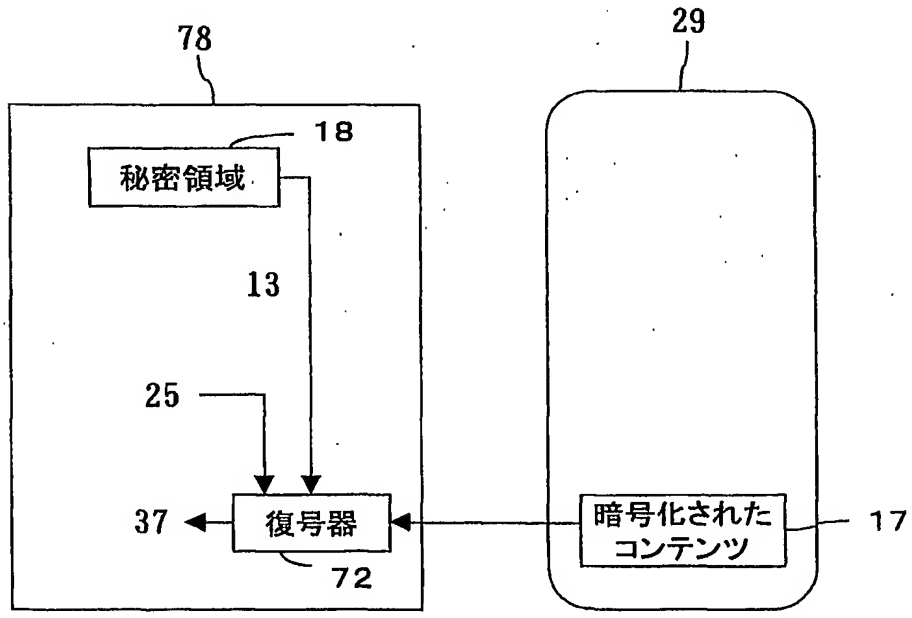
第１８（ｂ）図

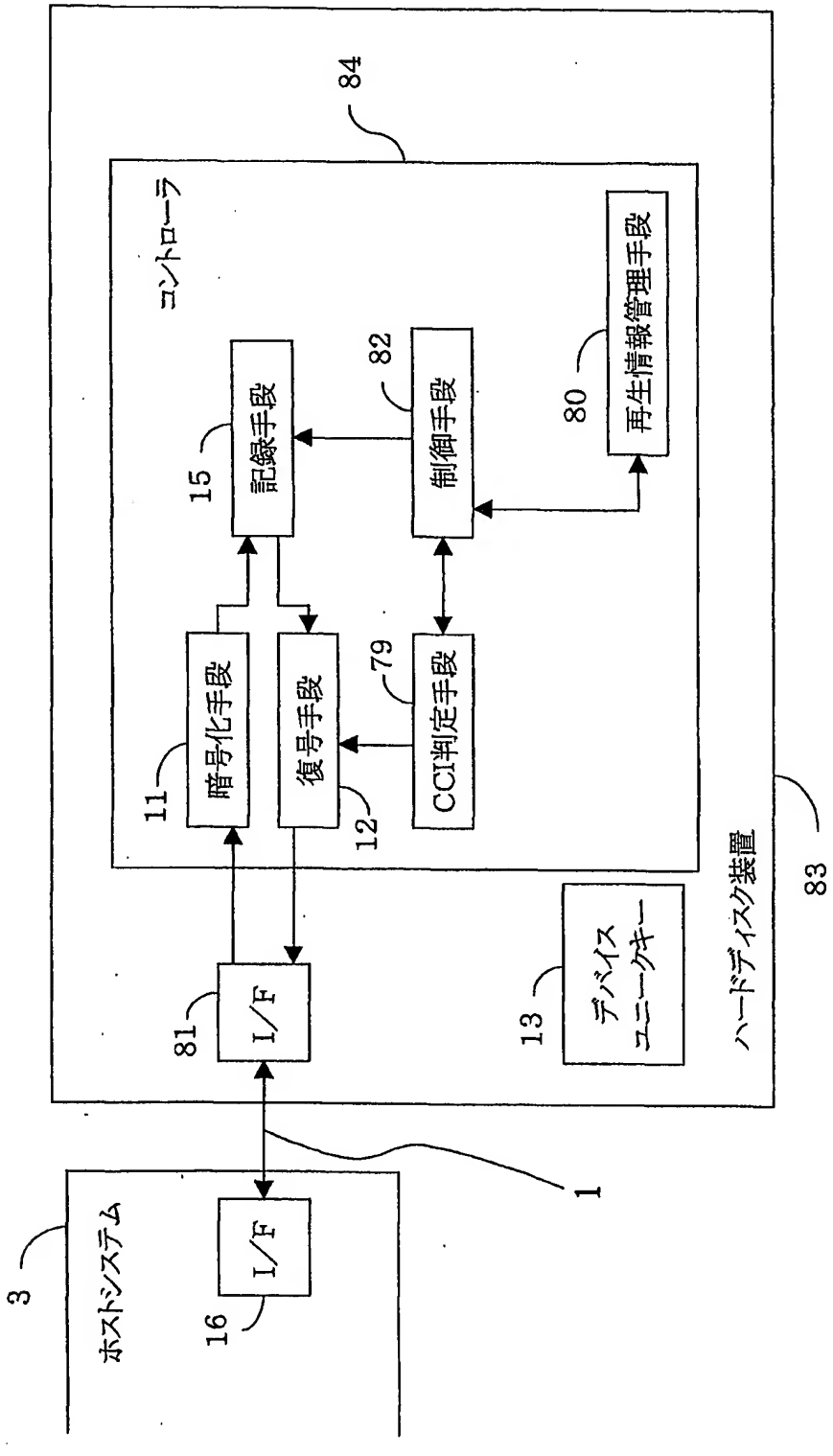

76
29
36
CCI
27
25
復号器
37
70
暗号化された
コンテンツ
17

第１９（ａ）図

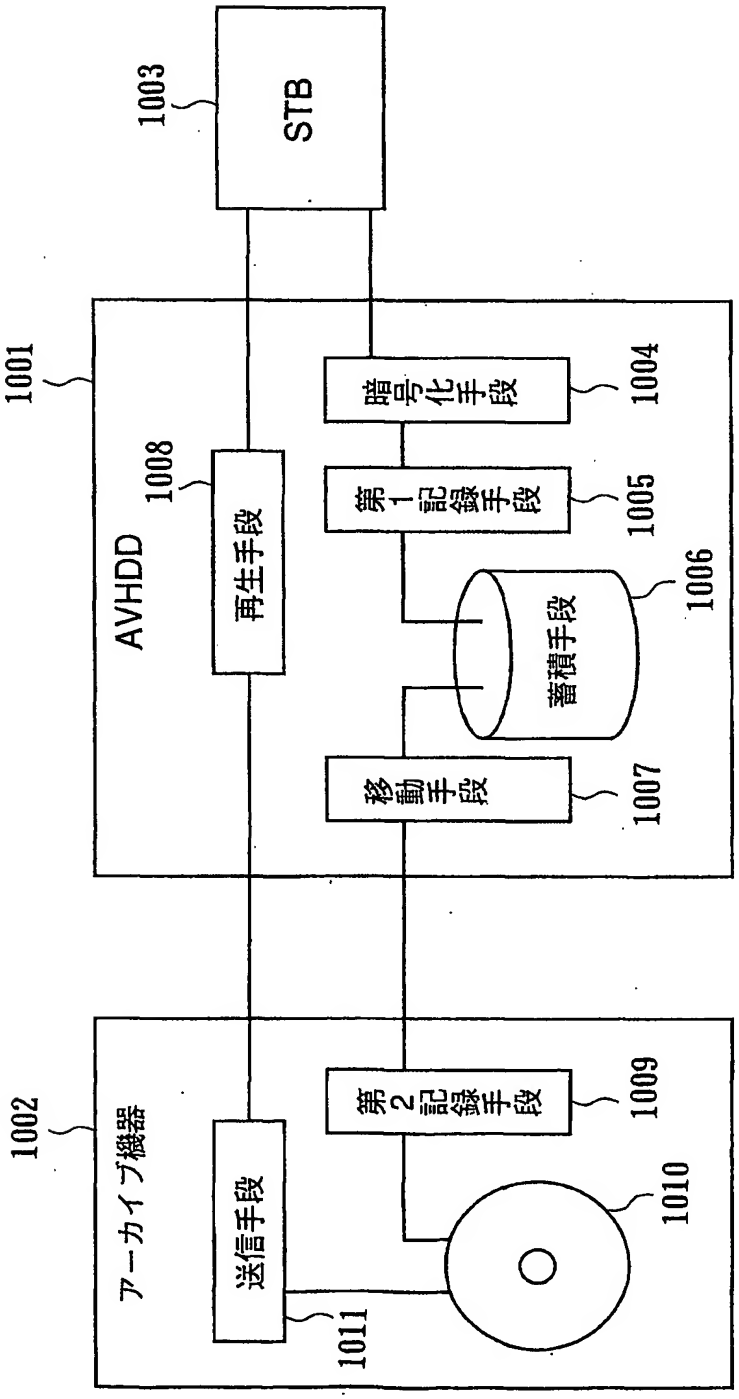

77
29
18
秘密領域
13
25
26
暗号器
71
暗号化された
コンテンツ
17

第１９（ｂ）図

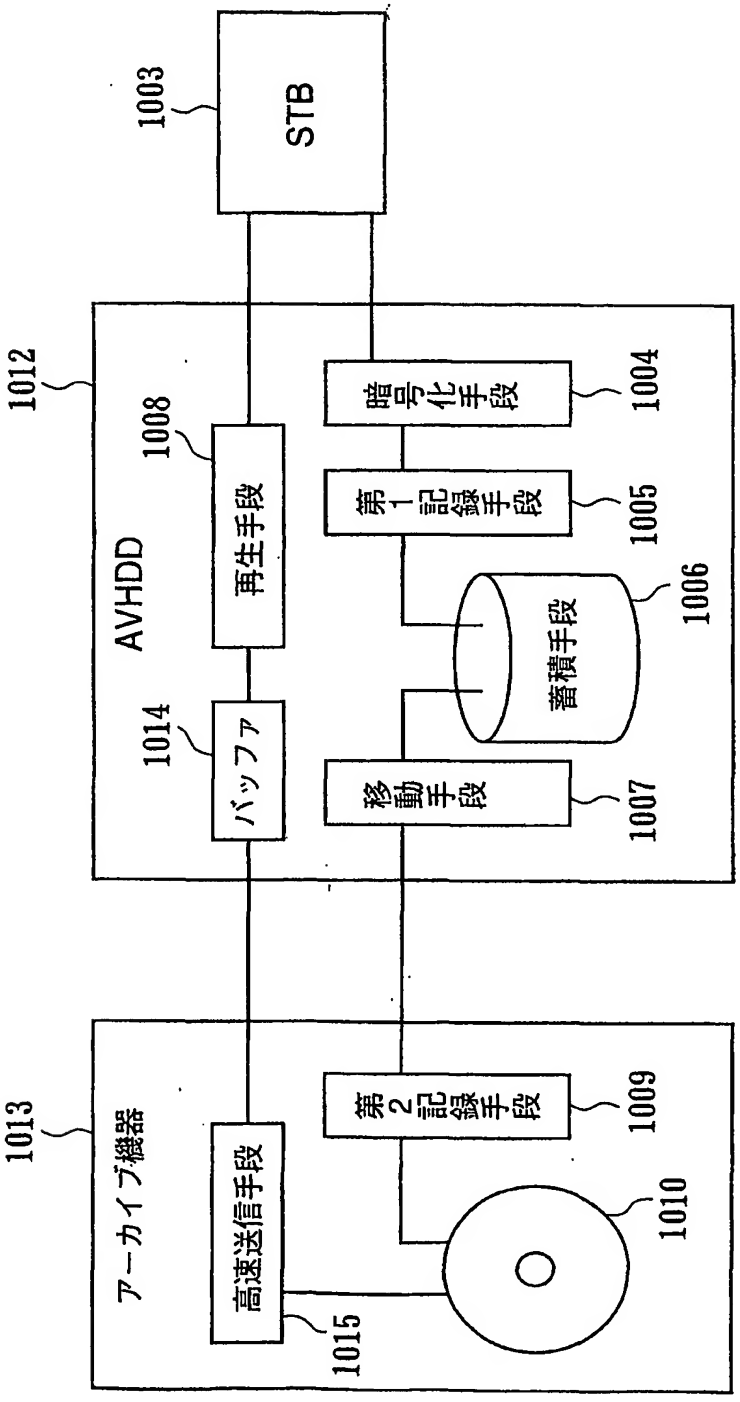

78
29
18
秘密領域
13
25
37
復号器
72
暗号化された
コンテンツ
17


84
コントローラ
15
記録手段
82
制御手段
80
再生情報管理手段
11
暗号化手段
12
復号手段
79
CCI判定手段
81
I/F
13
デバイス
ユニークキー
ハードディスク装置
83
1
3
ホストシステム
16
I/F

第２０図

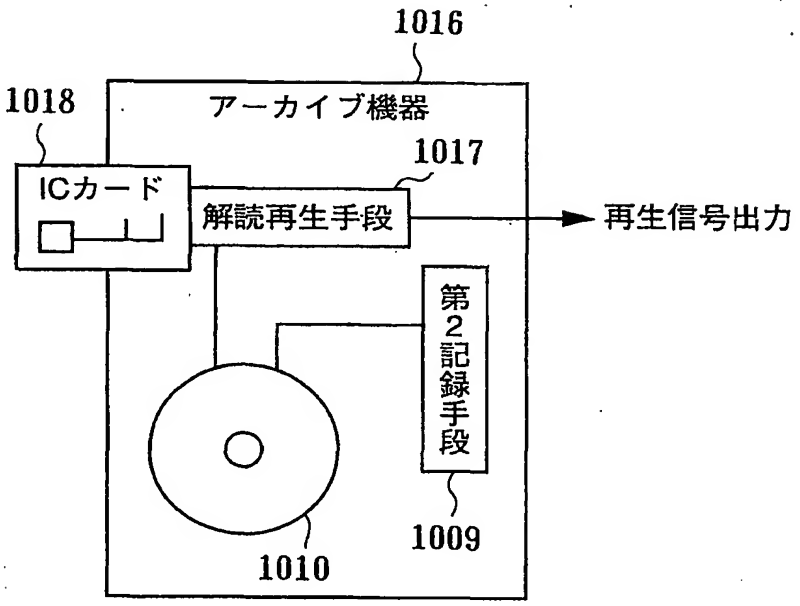

1003
STB
1001
AVHDD
1008
再生手段
暗号化手段
1004
第1記録手段
1005
蓄積手段
1006
移動手段
1007
1002
アーカイブ機器
送信手段
1011
第2記録手段
1009
1010

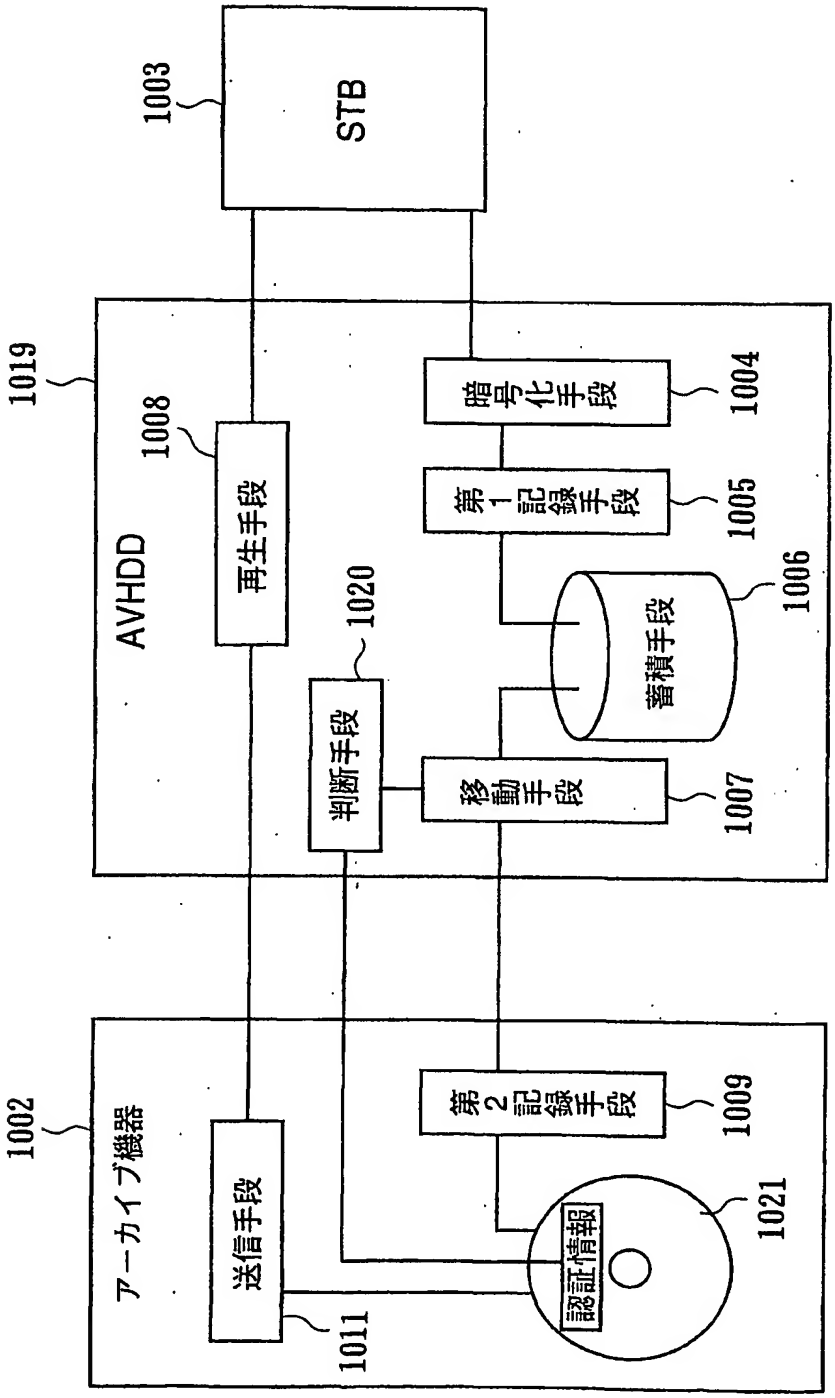
第２１図


1003
STB
1012
AVHDD
1008
再生手段
1014
バッファ
暗号化手段
1004
第1記録手段
1005
蓄積手段
1006
移動手段
1007
1013
アーカイブ機器
高速送信手段
1015
第2記録手段
1009
1010

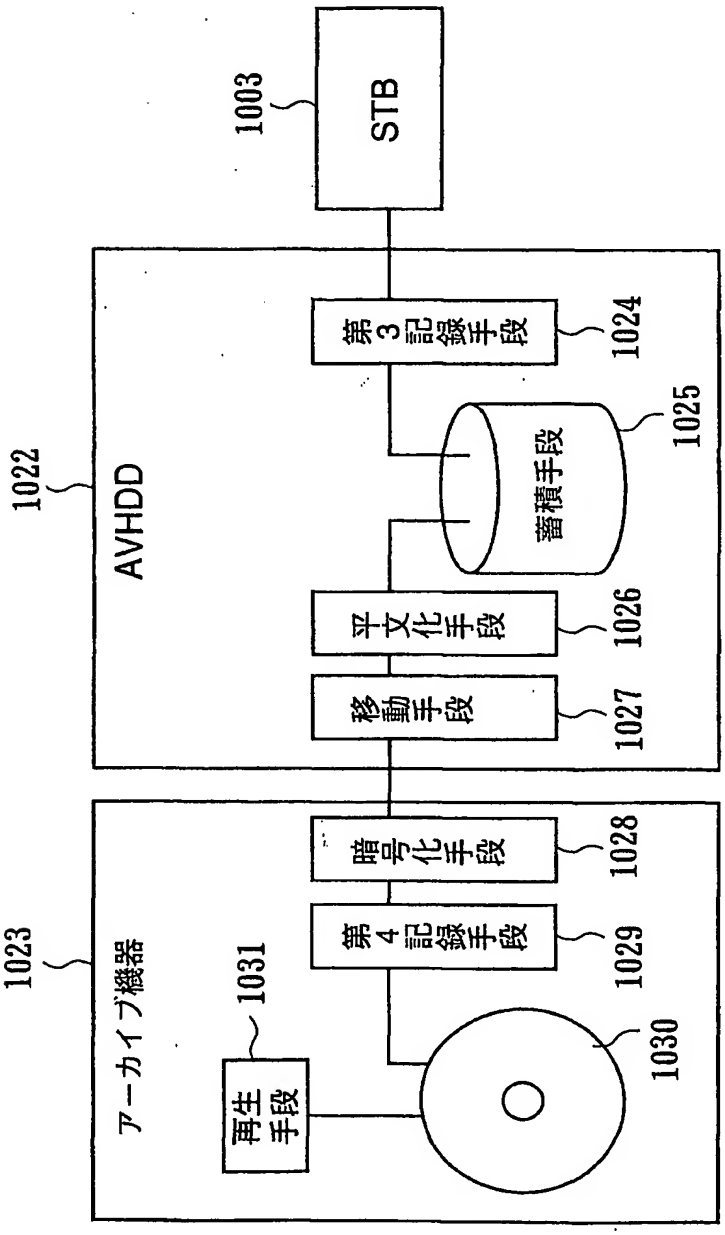
第２２図

第２３図


1016
1018
アーカイブ機器
1017
ICカード
解読再生手段
再生信号出力
第2記録手段
1009
1010

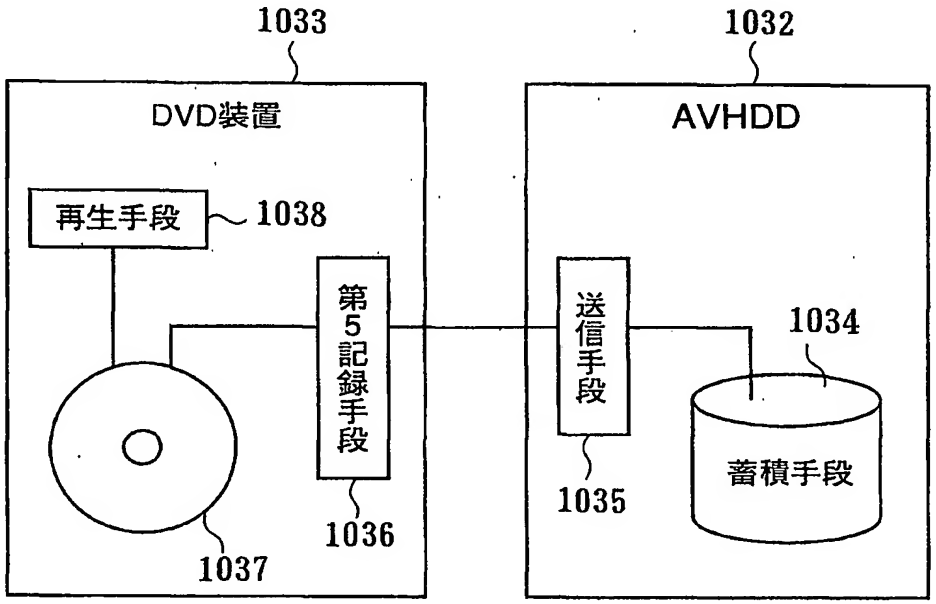

1003
STB
1019
AVHDD
1008
再生手段
暗号化手段
1004
第1記録手段
1005
蓄積手段
1006
1020
判断手段
移動手段
1007
1002
アーカイブ機器
送信手段
1011
第2記録手段
1009
認証情報
1021

第２４図

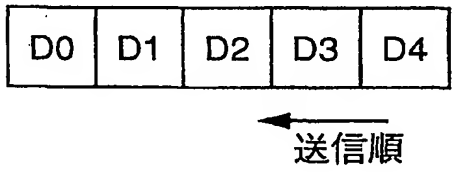

1003
STB
1022
AVHDD
第3記録手段
1024
蓄積手段
1025
平文化手段
1026
移動手段
1027
1023
アーカイブ機器
暗号化手段
1028
第4記録手段
1029
1031
再生手段
1030

第25図

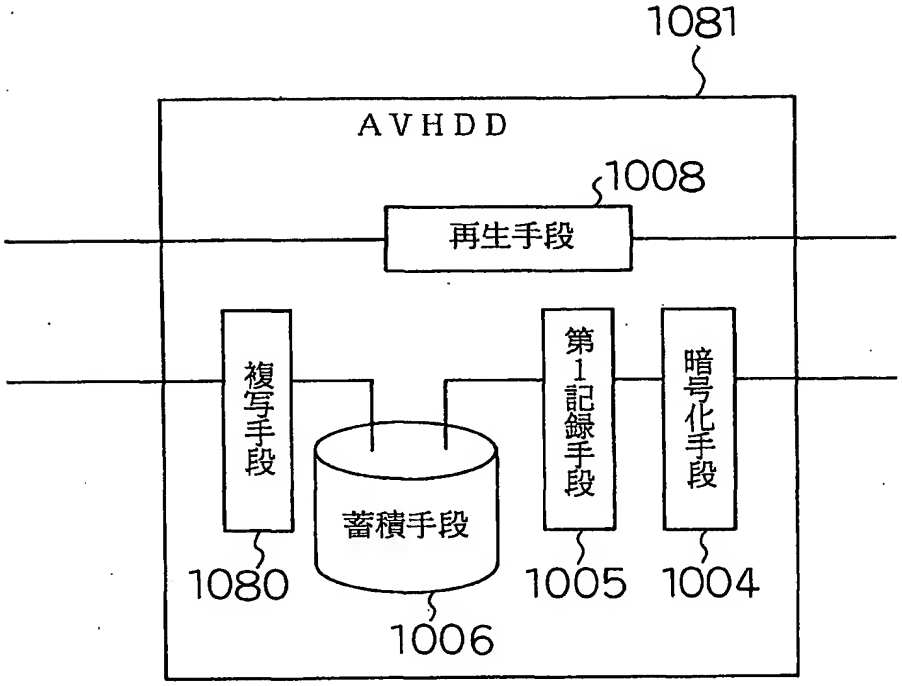
第２６図


1033
1032
DVD装置
AVHDD
再生手段
1038
第5記録手段
送信手段
1034
蓄積手段
1035
1036
1037

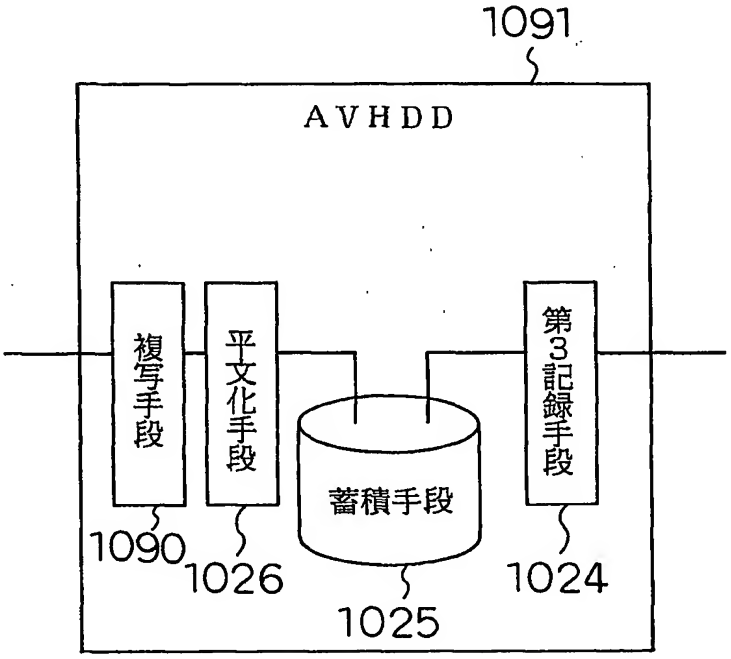
第２７図

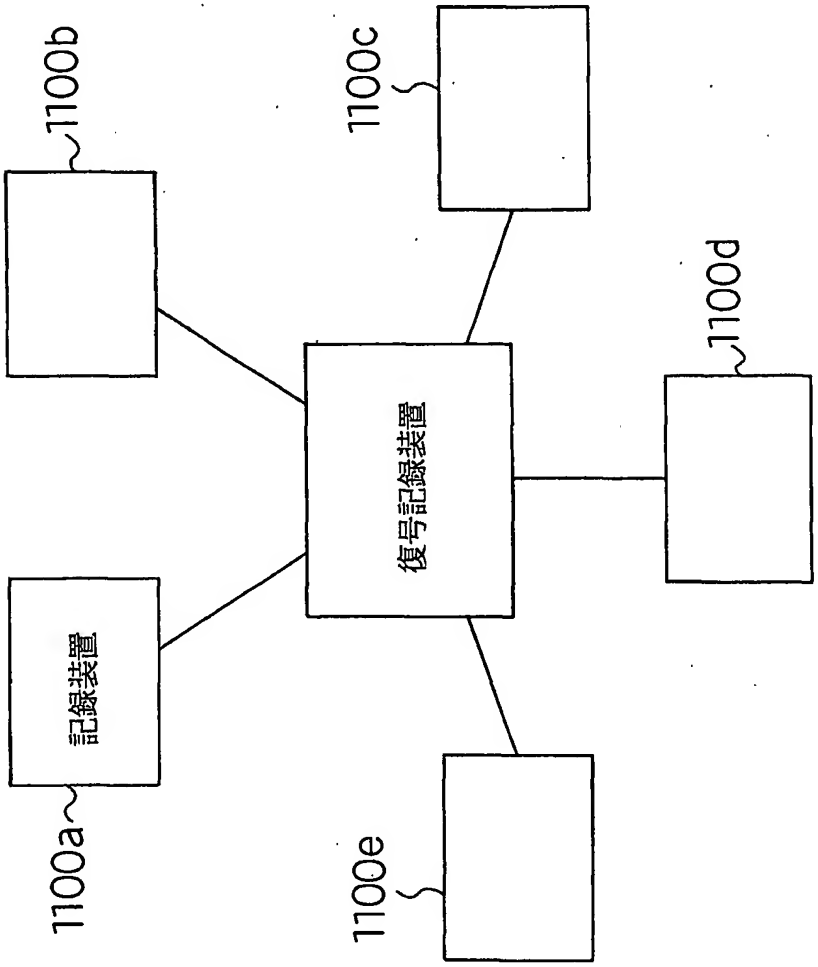

D0
D1
D2
D3
D4
送信順

第２８図


1081
AVHDD
1008
再生手段
複写手段
蓄積手段
第1記録手段
暗号化手段
1080
1006
1005
1004

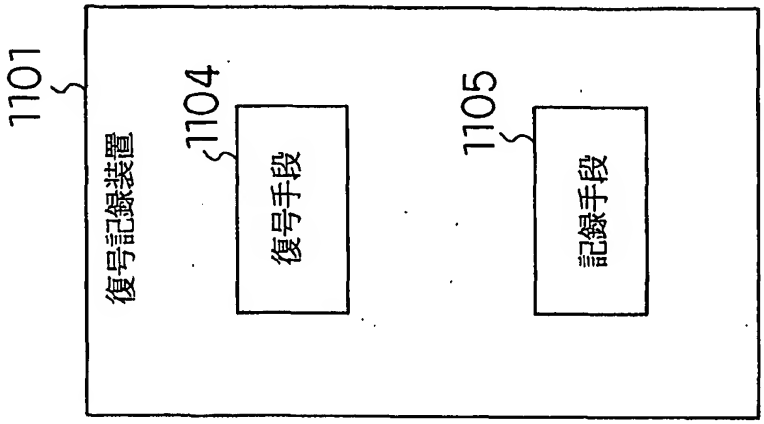
第２９図



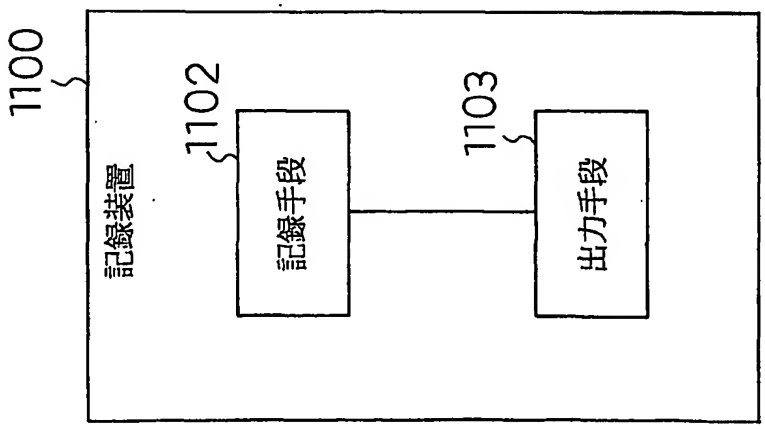


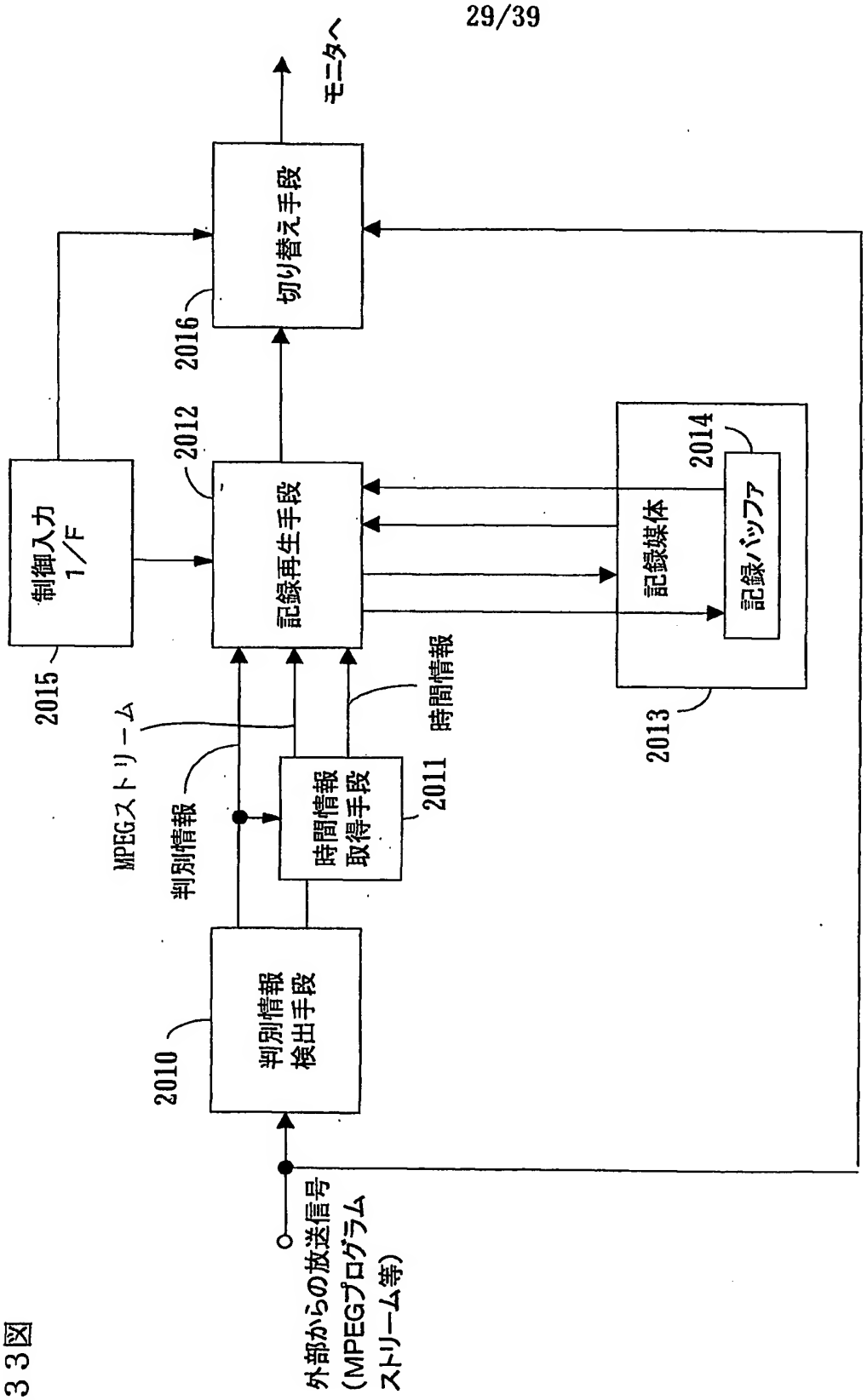
第３０図

第３２図


1101
復号記録装置
1104
復号手段
1105
記録手段

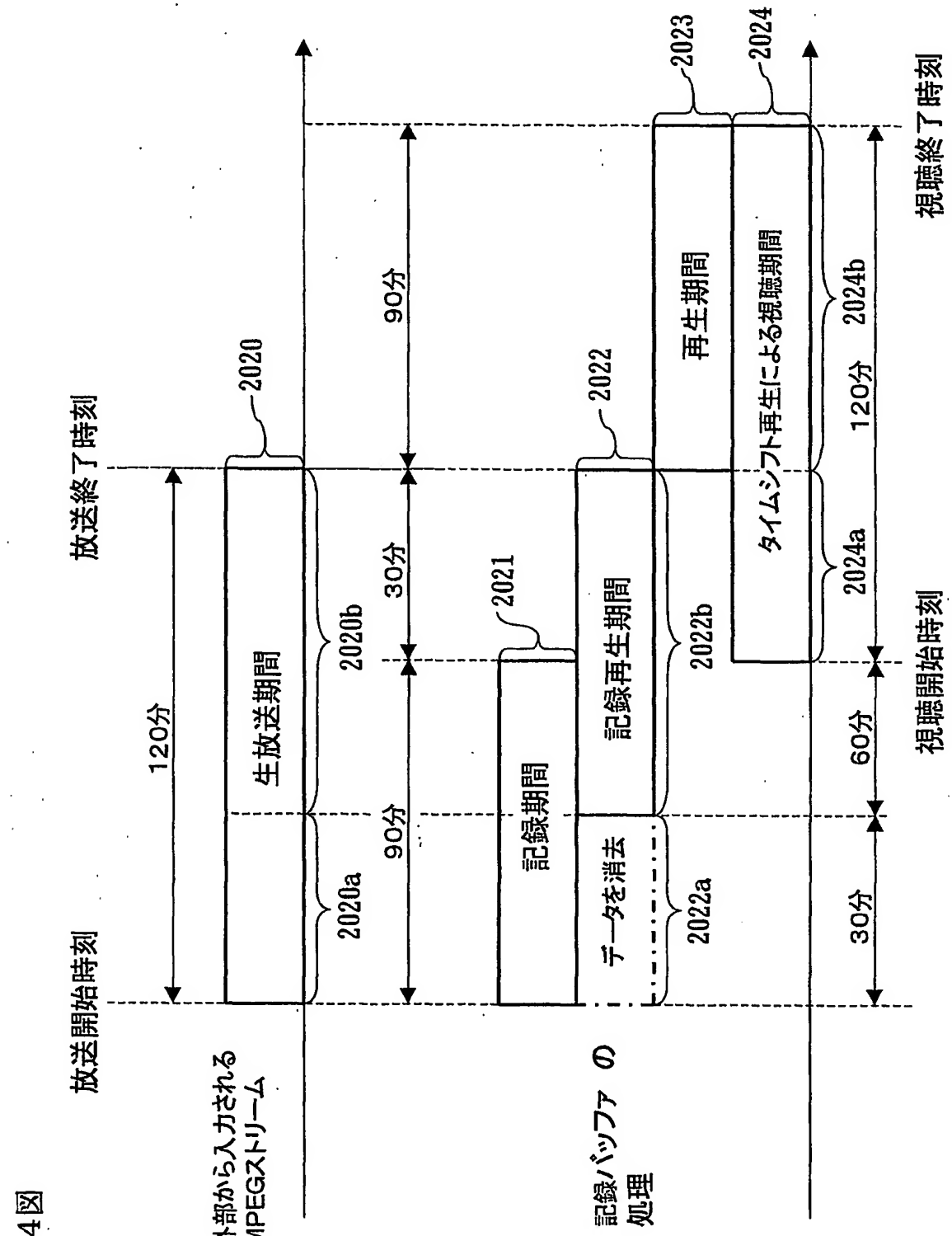
第３１図


1100
記録装置
1102
記録手段
1103
出力手段

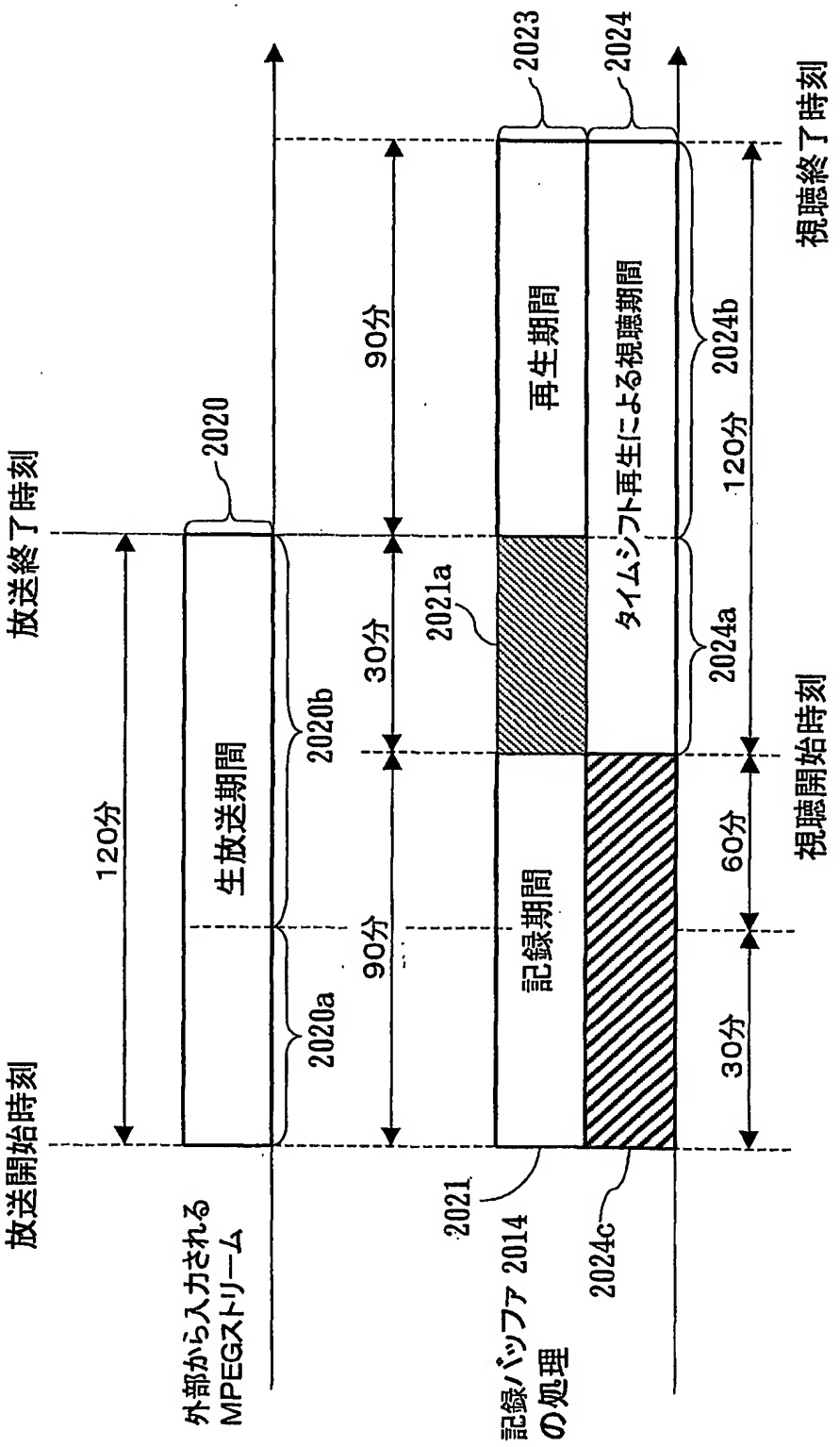

外部からの放送信号
(MPEGプログラム
ストリーム等)
判別情報
検出手段
2010
時間情報
取得手段
2011
MPEGストリーム
判別情報
時間情報
記録再生手段
2012
記録媒体
記録バッファ
2014
2013
制御入力
I/F
2015
切り替え手段
2016
モニタへ

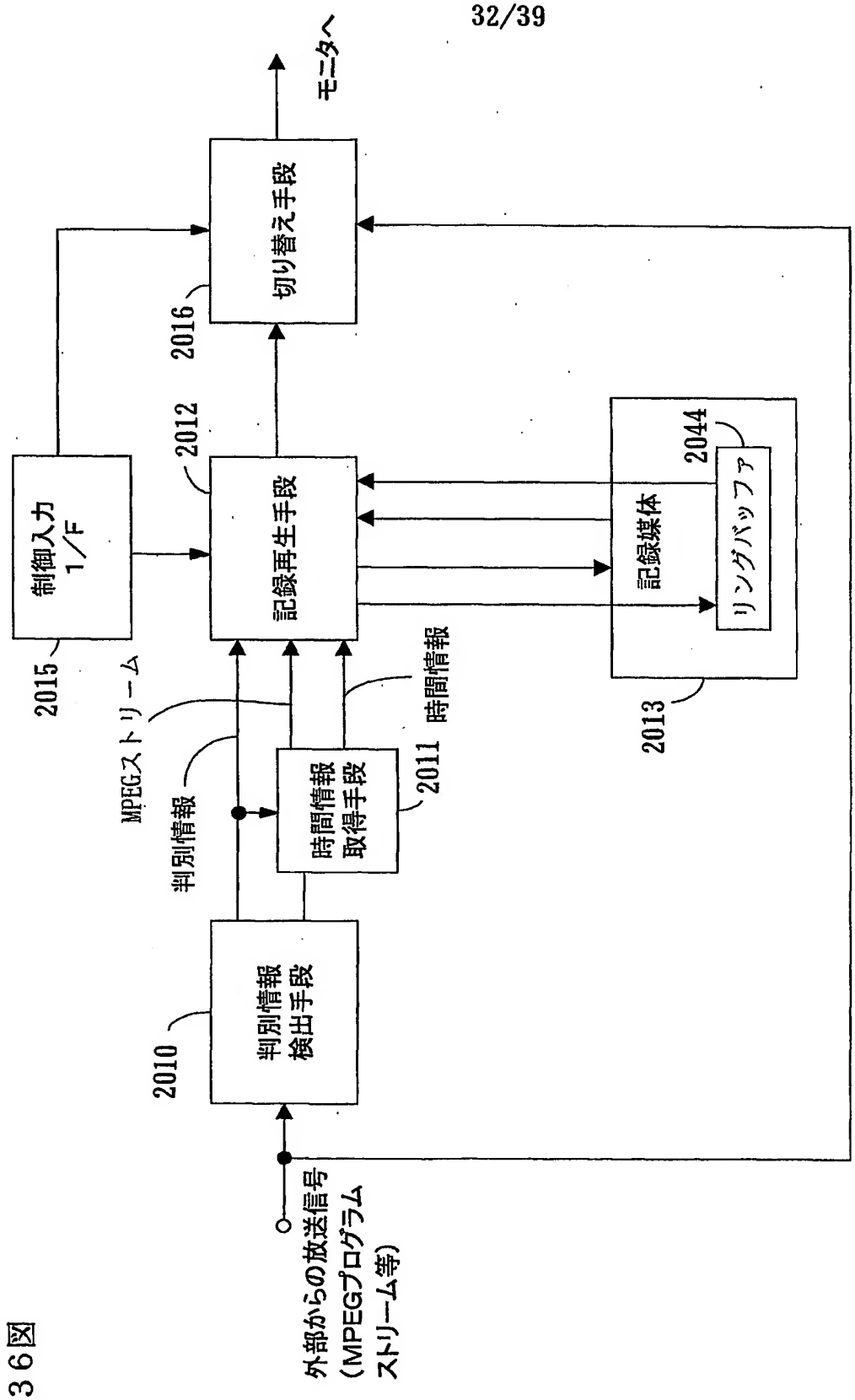
第３３図

第３４図


放送開始時刻
放送終了時刻
視聴開始時刻
視聴終了時刻
120分
90分
30分
90分
60分
30分
外部から入力されるMPEGストリーム
記録バッファの処理
生放送期間
2020
2020a
2020b
記録期間
2021
データを消去
記録再生期間
2022
2022a
2022b
再生期間
2023
タイムシフト再生による視聴期間
2024
2024a
2024b
120分

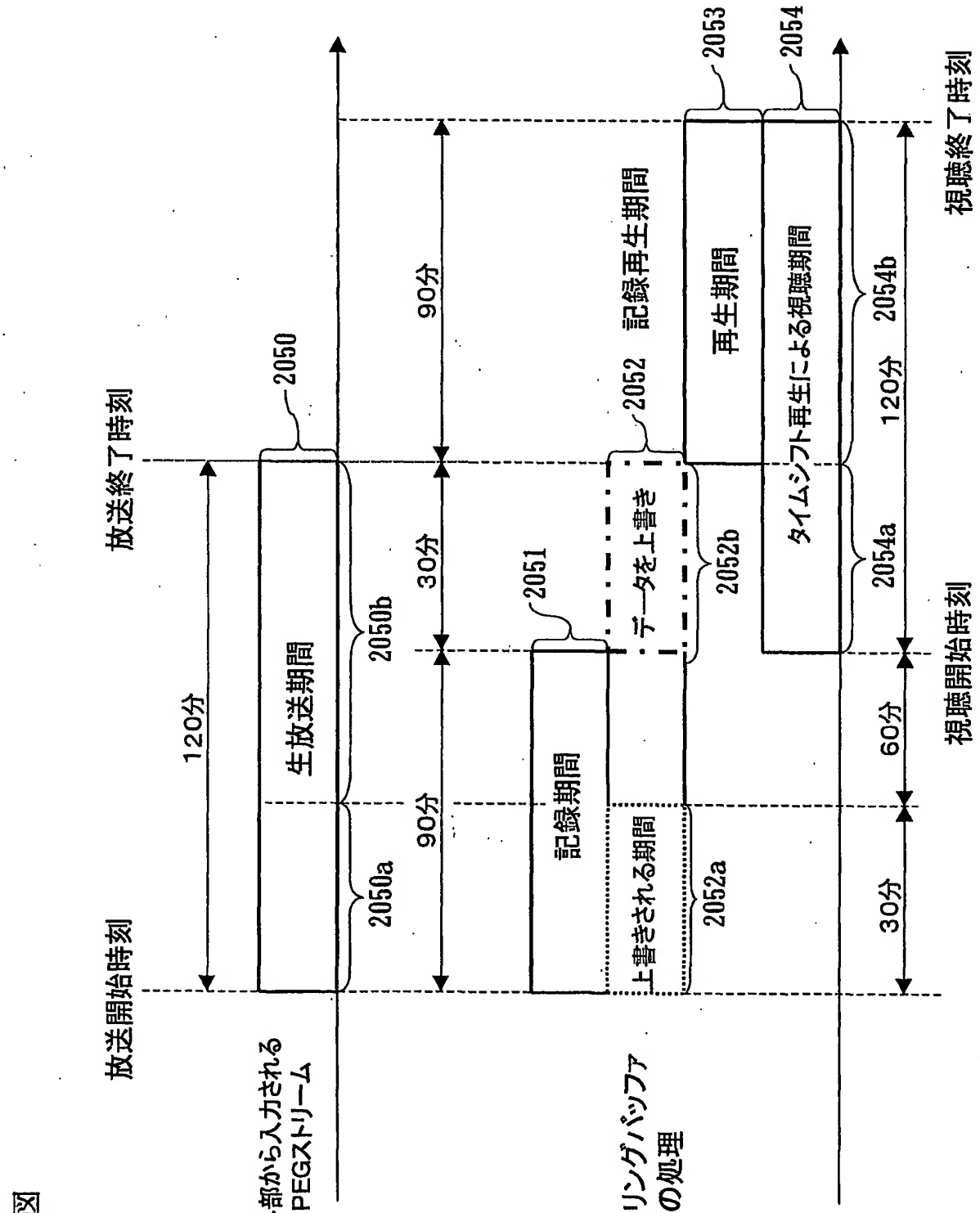
第３５図


放送終了時刻
放送開始時刻
120分
2020
生放送期間
2020b
2020a
90分
30分
90分
2021a
再生期間
記録期間
2023
2024
タイムシフト再生による視聴期間
2024b
2024a
120分
視聴終了時刻
視聴開始時刻
60分
30分
外部から入力されるMPEGストリーム
記録バッファ2014の処理
2021
2024c

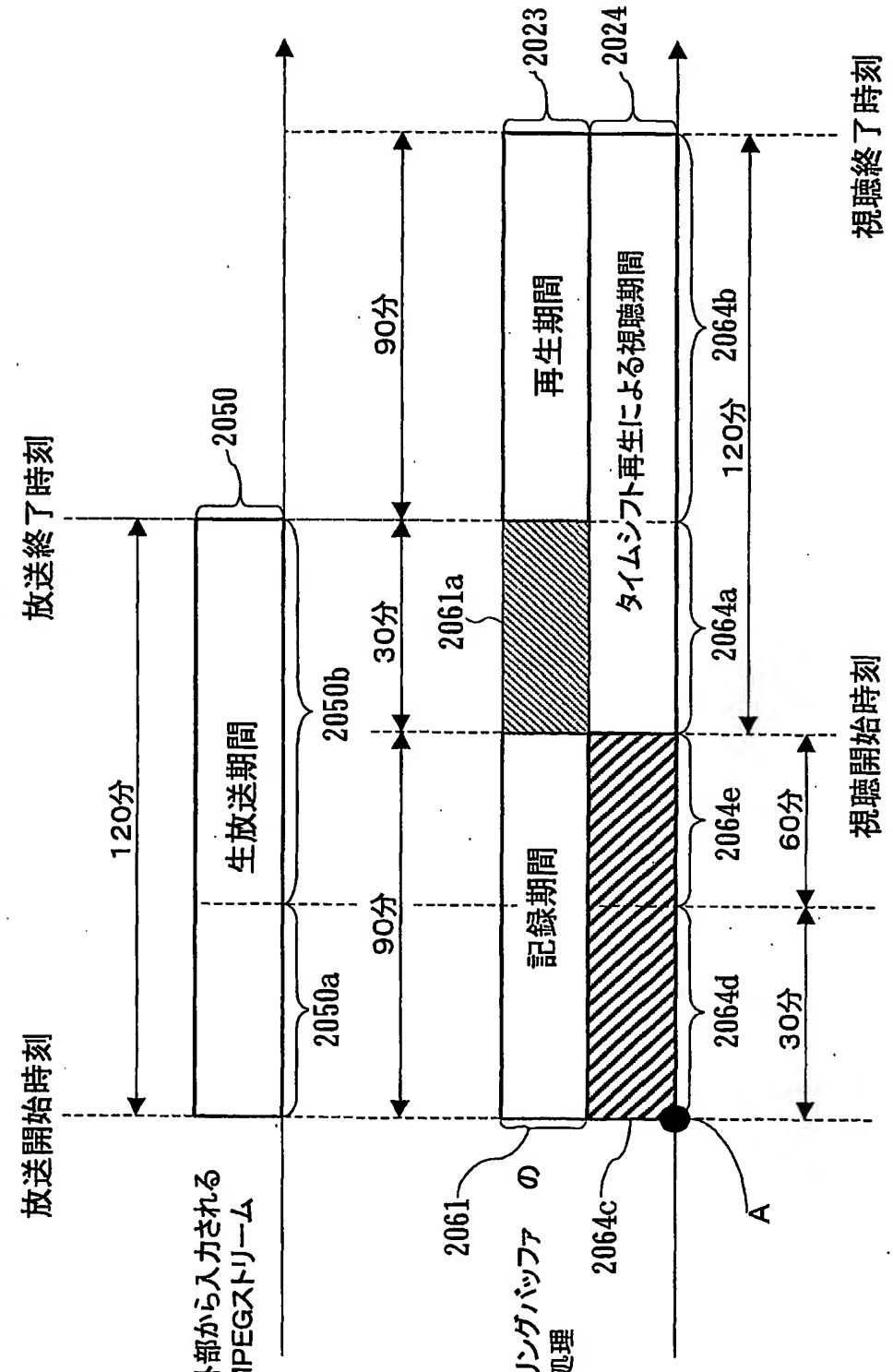

外部からの放送信号
(MPEGプログラム
ストリーム等)
2010
判別情報
検出手段
2011
時間情報
取得手段
判別情報
MPEGストリーム
時間情報
2012
記録再生手段
2013
記録媒体
2044
リングバッファ
2015
制御入力
I/F
2016
切り替え手段
モニタへ

第３６図

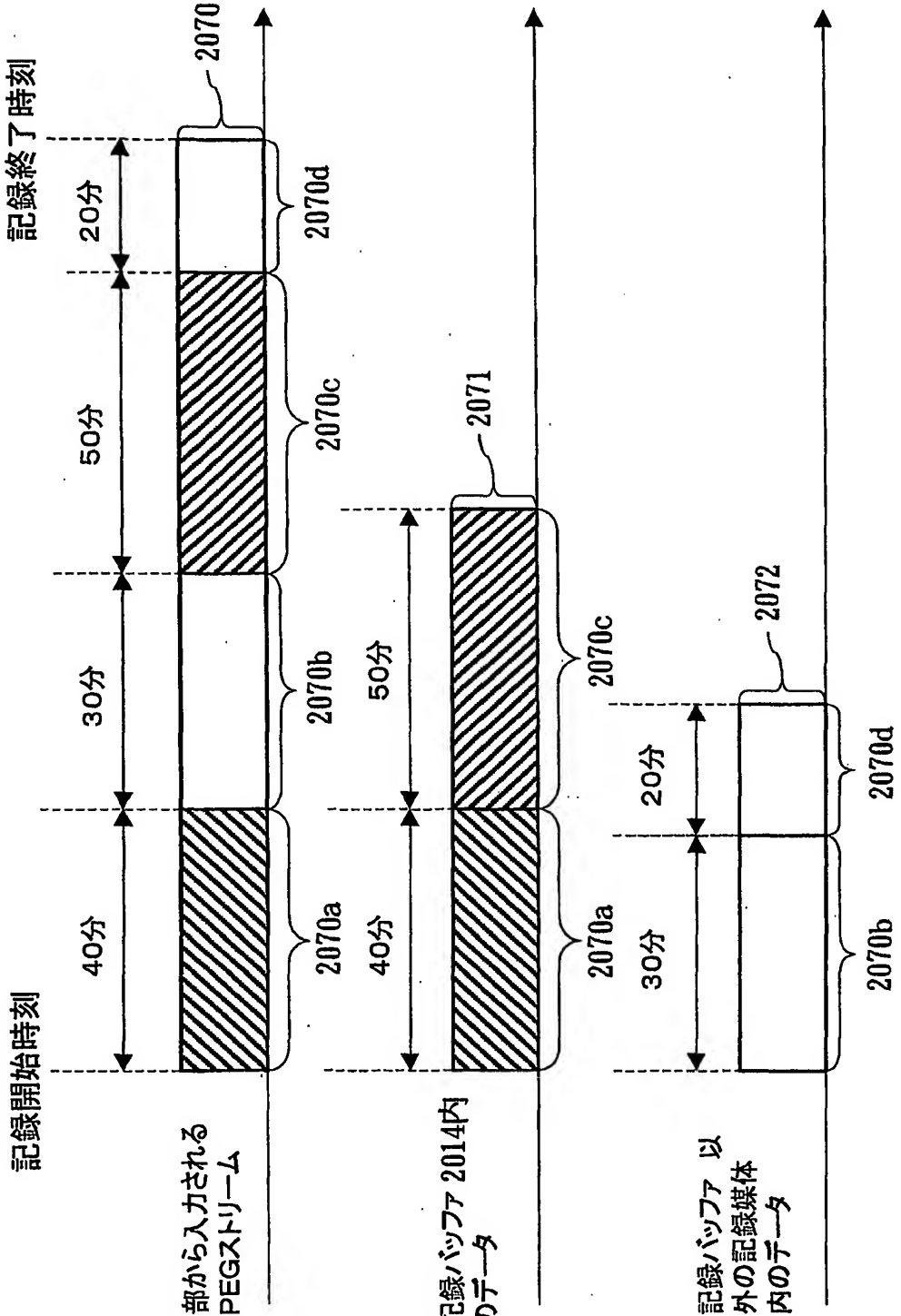
第３７図

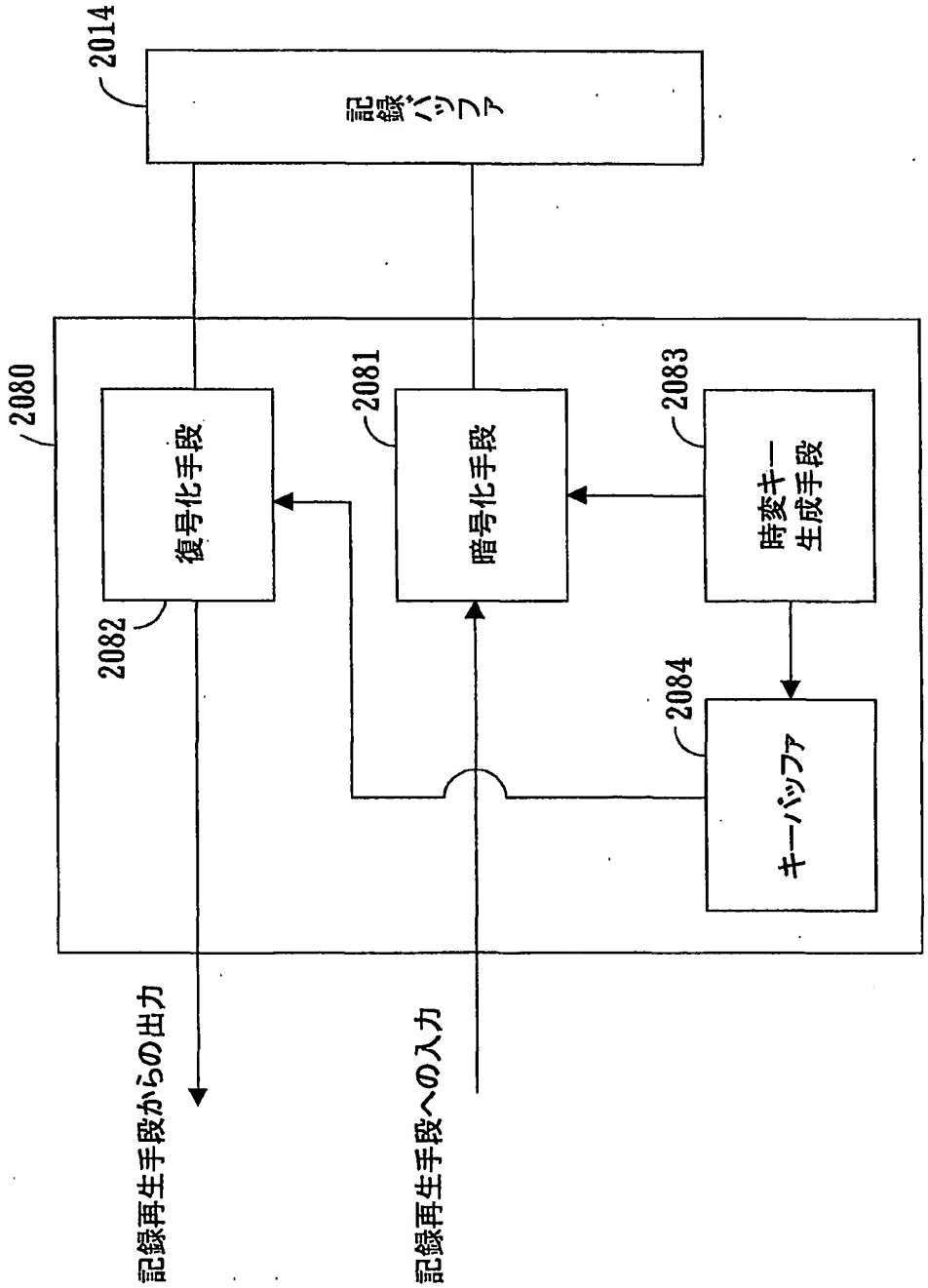

放送開始時刻
放送終了時刻
視聴開始時刻
視聴終了時刻
120分
90分
30分
60分
外部から入力されるMPEGストリーム
生放送期間
2050
2050a
2050b
リングバッファの処理
記録期間
2051
上書きされる期間
2052
2052a
2052b
データを上書き
記録再生期間
再生期間
2053
タイムシフト再生による視聴期間
2054
2054a
2054b

第３８図

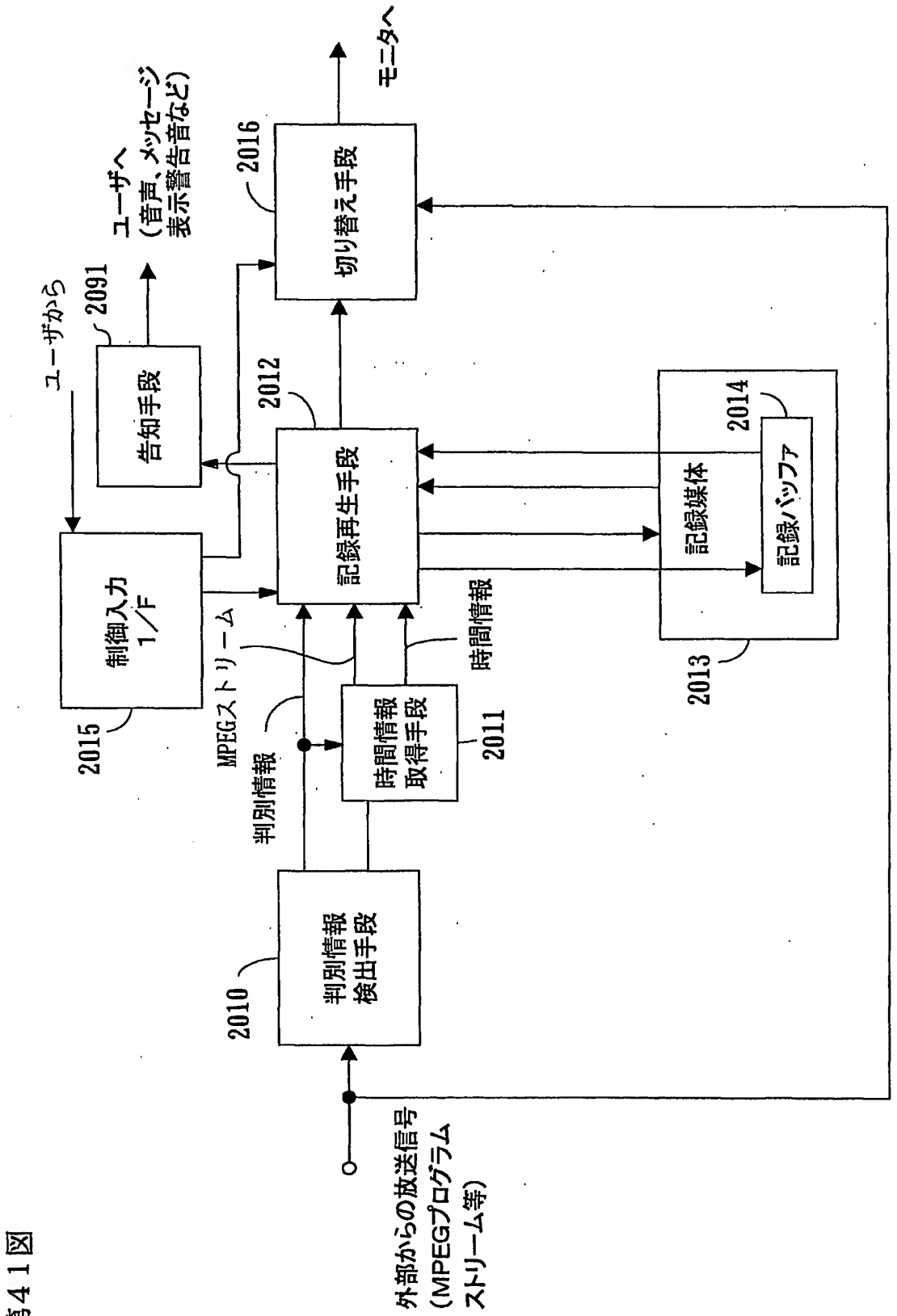

放送開始時刻
放送終了時刻
視聴開始時刻
視聴終了時刻
120分
90分
30分
60分
2050
2050a
2050b
生放送期間
2061
2061a
記録期間
2023
2024
再生期間
タイムシフト再生による視聴期間
2064a
2064b
2064c
2064d
2064e
外部から入力されるMPEGストリーム
リングバッファの処理
A

第３９図


記録開始時刻
記録終了時刻
40分
30分
50分
20分
2070a
2070b
2070c
2070d
2070
2071
2072
外部から入力されるMPEGストリーム
記録バッファ 2014内のデータ
記録バッファ 以外の記録媒体内のデータ

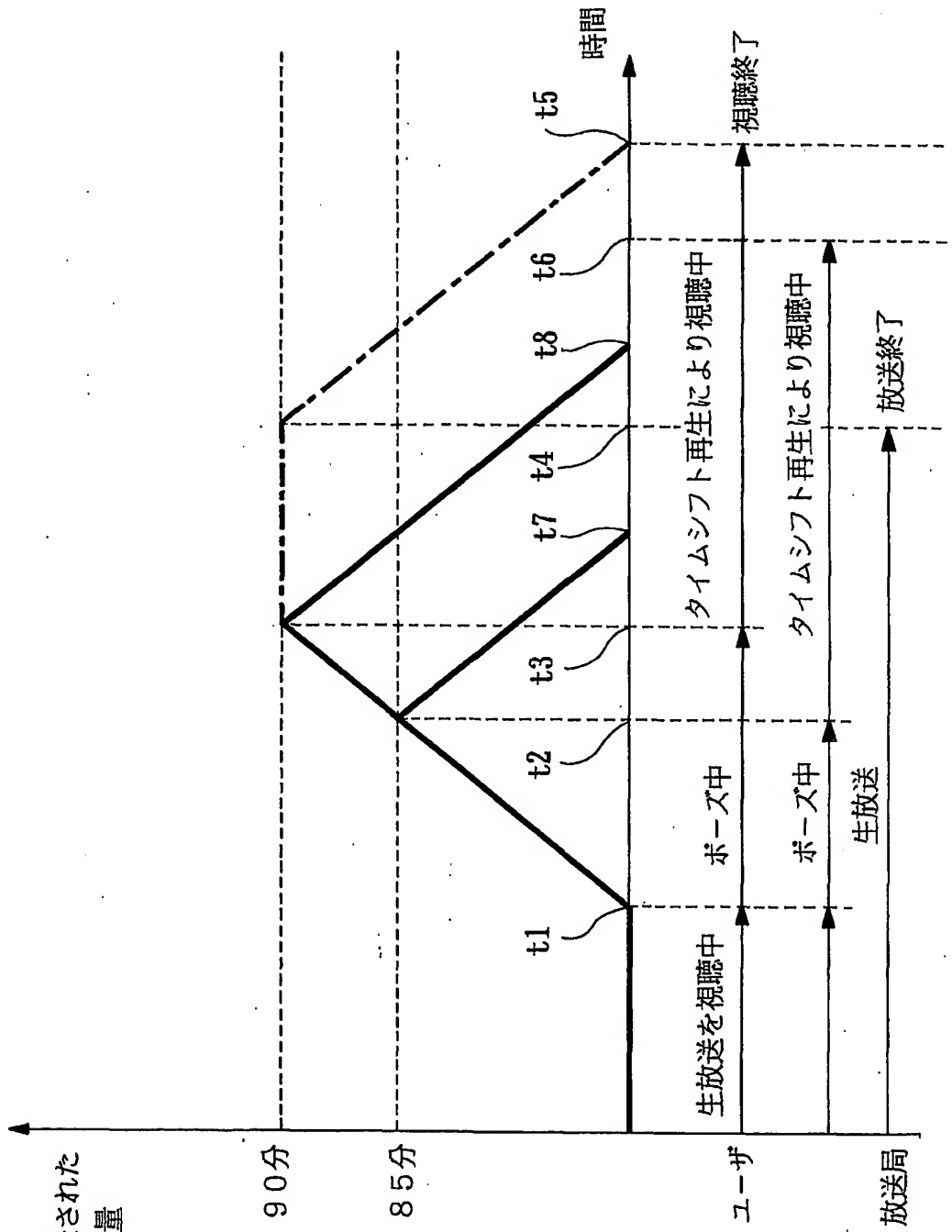

2014
記録バッファ
2080
復号化手段
2081
暗号化手段
2083
時変キー生成手段
2082
2084
キーバッファ
記録再生手段からの出力
記録再生手段への入力

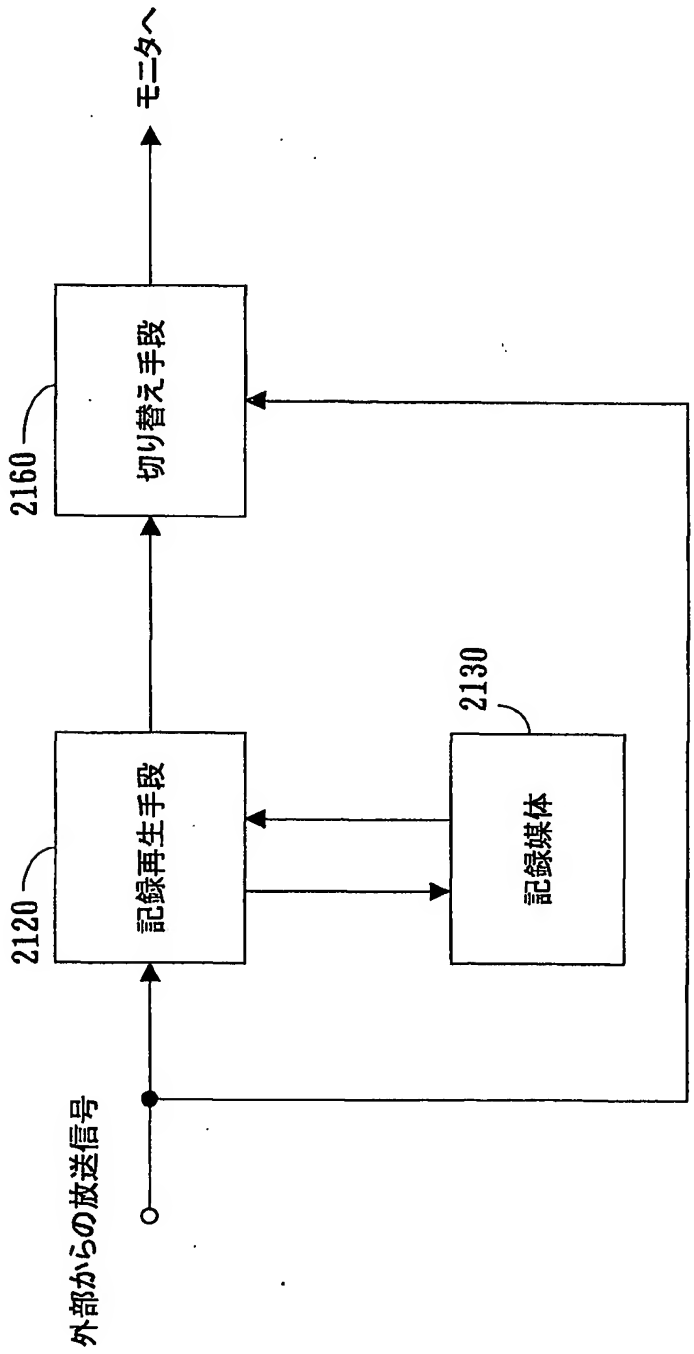
第４０図


外部からの放送信号
(MPEGプログラム
ストリーム等)
2010
判別情報
検出手段
判別情報
MPEGストリーム
時間情報
取得手段
2011
時間情報
2013
記録媒体
2014
記録バッファ
記録再生手段
2012
切り替え手段
2016
モニタへ
ユーザへ
(音声,メッセージ
表示警告音など)
2091
告知手段
ユーザから
制御入力
I/F
2015

第４１図

第４２図


記録バッファに一時記録された
複製禁止コンテンツの残量
９０分
８５分
ユーザ
放送局
時間
t1
t2
t3
t4
t5
t6
t7
t8
生放送を視聴中
ポーズ中
生放送
タイムシフト再生により視聴中
タイムシフト再生により視聴中
視聴終了
放送終了



第４３図

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09260

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B 20/10, G11B 20/12, G06F 17/60, G06F 3/06, H04N 5/91, H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B 20/10, H04N 5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-149619, A (Victor Company of Japan, Limited), 02 June, 1998 (02.06.98), Full text; Figs. 1 to 4 (Family: none)	1-74
Y A	JP, 10-40639, A (Sony Corporation), 13 February, 1998 (13.02.98), Full text; Figs. 1 to 5 (Family: none)	1-74 75
Y	JP, 11-86437, A (Toshiba Corporation), 30 March, 1999 (30.03.99), Full text; Figs. 1 to 8 (Family: none)	1-74
Y	JP, 9-191453, A (Sony Corporation), 22 July, 1997 (22.07.97), Full text; Figs. 1 to 16 & EP, 000740478, A2 & KR, 000231391, B & US, 006163644, A	76-95
Y	JP, 8-297919, A (Kabushiki Kaisha Hitachi Seisakusho Personal Media Kiki Jigyoubu), 12 July, 1996 (12.07.96), Full text; Figs. 1 to 10 (Family: none)	76-95

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April, 2001 (10.04.01)	24 April, 2001 (24.04.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09260

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 11-164254, A (Sony Electronics Inc.), 18 June, 1999 (18.06.99), Full text; Figs. 1 to 4 & NL, 001010109, A & GB, 002329997, A & DE, 019844635, A & GB, 009820939, A0	76-95
Y	JP, 10-56620, A (Matsushita Electric Ind. Co., Ltd.), 24 February, 1998 (24.02.98), Full text; Figs. 1 to 74 & EP, 000789488, A2 & CN, 001171012, A & US, 005999691, A1	85,86, 89,90

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09260

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See the extra sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09260

Continuation of Box No.II of continuation of first sheet (1)

The inventions of claims 1-21, 30-44 relate to an idea of recording copyright protection data on an HDD.

The inventions of claims 22-29 relate to an arrangement on a printed board.

The inventions of claims 45-75 relate to an idea of transferring/copying copyright protection data recorded on an HDD to another device.

The inventions of claims 76-95 relate to an idea of time-shift reproduction of copyright protection data recorded on an HDD.

国際調査報告 | 国際出願番号 PCT／JP00／09260

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G11B 20/10、G11B 20/12、G06F 17/60、G06F 3/06、H04N 5/91、H04L 9/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G11B 20／10 、H04N 5/91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2001年
日本国登録実用新案公報 1994－2001年
日本国実用新案登録公報 1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 10-149619, A（日本ビクター株式会社） 2. 6月. 1998 (02. 06. 98) 全文 第1－4図（ファミリーなし）	1-74
Y A	JP, 10-40639, A（ソニー株式会社） 13. 2月. 1998 (13. 02. 98) 全文 第1－5図（ファミリーなし）	1-74 75

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 10. 04. 01	国際調査報告の発送日 24.04.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 宮下 誠 印 5Q 2946 電話番号 03－3581－1101 内線 3589

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告 国際出願番号 PCT／JP00／09260

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 11-86437, A (株式会社東芝) 30. 3月. 1999 (30. 03. 99) 全文 第1－8図 (ファミリーなし)	1-74
Y	JP, 9-191453, A (ソニー株式会社) 22. 7月. 1997 (22. 07. 97) 全文 第1－16図 & EP, 000740478 , A2 & KR, 000231391 , B & US, 006163644 , A	76-95
Y	JP, 8-297919, A (株式会社日立製作所パーソナルメディア機器事業部) 12. 7月. 1996 (12. 07. 96) 全文 第1－10図 (ファミリーなし)	76-95
Y	JP, 11-164254, A (ソニーエレクトロニクス インク) 18. 6月. 1999 (18. 06. 99) 全文 第1－4図 & NL, 001010109 , A & GB, 002329997 , A & DE, 019844635 , A & GB, 009820939 , A0	76-95
Y	JP, 10-56620, A (松下電器産業株式会社) 24. 2月. 1998 (24. 02. 98) 全文 第1－74図 & EP, 000789488 , A2 & CN, 001171012 , A & US, 005999691 , A1	85、86、89、90

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ００／０９２６０

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

発明の単一性が欠如している理由は特別ページに記載した。

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報告 | 国際出願番号 ＰＣＴ／ＪＰ００／０９２６０

請求の範囲1-21、30-44に係る発明は、ＨＤＤへの著作権保護データの記録に関するものである。

請求の範囲22-29に係る発明は、プリント基板上の配置に関するものである。

請求の範囲45-75に係る発明は、ＨＤＤに記録された著作権保護データの他の機器への移動・複製に関するものである。

請求の範囲76-95に係る発明は、ＨＤＤに記録された著作権保護データのタイムシフト再生に関するものである。